Chapter 67

Improving Privacy and Security of User Data in Location Based Services

Mohammad Yamin
Department of Management Information Systems, King Abdulaziz University Jeddah, Saudi Arabia

Adnan Ahmed Abi Sen
Department of Computer Science, King Abdulaziz University, Jeddah, Saudi Arabia

ABSTRACT

Location Based Services (LBS) expose user data to malicious attacks. Approaches, evolved, so far, for preserving privacy and security, suffer from one or more anomalies, and hence the problem of securing LBS data is far from being resolved. In particular, accuracy of results vs. privacy degree, privacy vs. performance, and trust between users are open problems. In this article, we present a novel approach by integration of peer-to-peer (P2P) with the caching technique and dummies from real queries. Our approach increases efficiency, leads to improved performance, and provides solutions to many problems that have existed in the past. In addition, we offer an improved way of managing cache. Simulation demonstrates superiority of our approach over earlier ones dealing with both the ratio of privacy and that of performance.

INTRODUCTION

Digital revolution, resulting in a large-scale innovation and development in the field of communications, has contributed to the phenomenal increase in the internet based tools, devices and applications. Availability of stable, fast and reliable internet services has led to provision of new services aimed at improving our life style. For example, GPS technology and tools are being used by the corporate world to resolve and answer a huge number of queries about the locations of the points of interests (POI) for static and moving objects. The GPS is also being used extensively in commercial fields such as directing adver-

DOI: 10.4018/978-1-7998-8954-0.ch067

tisements to potential users, and searching number (k) of nearest neighbors, destinations, customers or objects. Many of these as well as other applications are dependent on the location based services (LBS).

Despite big benefits that are provided by LBS, there is a growing concern about preserving privacy of users raising or initiating a query. This is because, at the time of initiating a query and its subsequent propagation, there is a considerable probability of a third party (scrupulous or malicious) to detect and hack the information about the identity of the users, details of their characters, habits, beliefs, and personal information. In a virtual environment, an attacker can prevail and monitor the victim (user). In some cases, service providers could themselves be accomplices of hackers. There are several approaches in the literature dealing with preserving privacy and security of data in LBS. Main approaches, six of them, are the ones dealing with concepts of Dummies, K-anonymity and Trusted Third Parties (TTP), Obfuscation, Private Information Retrieval (PIR), Cooperation between users and Caching. All of these approaches suffer from serious anomalies and the problem of securing data in LBS server is far from being resolved. More details are provided by Bettini, Mascetti, Wang, Freni and Jajodia (2009), Wernke, Skvortsov, Dürr and Rothermel (2014), and Theodorakopoulos (2015).

In this article, we introduce a new approach for privacy and security of the users' data treated by LBS server. Our approach is based on the concept of cooperation between peers (P2P), facilitated by cache and then integration with what we term as real dummies. Before providing detailed description of our approach, we first give an account of the six approaches and an overview of earlier results.

LITERATURE REVIEW

Maintaining privacy and keeping data secure has always been a very challenging issue for the IT industry. These issues in the context of big data are thoroughly discussed by Tamane, S., Solanki, V. K., and Dey, N. (2017). In this article, our focus is on the Privacy and security of data in LBS processing, which can be breached by a hacker from outside or within. A hacker could be a user of LBS or server maintenance personnel. Here we summarise the six approaches which have so far been evolved to overcome this threat. A general classification for privacy protection methods including an account of the attacker knowledge is provided by Wernke, Skvortsov, Dürr and Rothermel (2014).

Classification of Approaches for Preserving Privacy of LBS Servers

As mentioned earlier, exiting methods and approaches of privacy and security of LBS server data can be combined into six approaches. We claim that our approach is an improvement over these approaches, which are describe here.

Obfuscation and Mix Zone

When a query is initiated, user's exact location is not communicated to the LBS server. Instead the user corrupts his location (in the Obfuscation) or transmits his/her nickname to LBS server, and this nickname is changed in each Zone. This is done by means of some mathematical transformations. This method was introduced by Duckham, Matt, and Lars (2005), and Ardagna, Cremonini, Damiani, Di, and Samarati (2007), which archives the objective of hiding the user's location but at the cost of compromising the degree of accuracy of the answer of the query. There are other drawbacks in this process, which are

Related Content