Abstract

Mobile devices users in Participatory Sensing Systems (PSS) are required to collect information from their nearby data collection points (DCs). A query normally reveals the identity (id), location, and user profile (e.g., race domain). This information facilitates an adversary PS server to infer over time a comprehensive user location summary with a high degree of precision. Some privacy techniques in PSS have been suggested recently to provide user privacy protection. However, only a few techniques that consider trust in static objects but disregard profile information. For credibility of data, there is scarcely any service, which entails the user to prove that she is at a particular DC point at a certain time. Yet none of the position and time information achieved by nowadays mobile devices is reliable. In this paper, we propose an enhanced K-location privacy-aware framework for static objects in PS system. The experimental results demonstrate in our approach user a high degree of anonymity and reliability of collected data.

References


Index Terms

Computer Science

Information Sciences

Keywords

Privacy, Anonymity, location attacks, profile, Visibility