Privacy-Preserving Indoor Localization on Smartphones

Abstract

WiFi-based positioning systems have recently received considerable attention, mainly because GPS is unavailable in indoor spaces and consumes considerable energy. On the other hand, predominant Smartphone OS localization subsystems currently rely on server-side localization processes, allowing the service provider to know the location of a user at all times. In this paper, we propose an innovative algorithm for protecting users from location tracking by the localization service, without hindering the provisioning of fine-grained location updates on a continuous basis. Our proposed Temporal Vector Map (TVM) algorithm, allows a user to accurately localize by exploiting a $k$-Anonymity Bloom ($kAB$) filter and a bestNeighbors generator of camouflaged localization requests, both of which are shown to be resilient to a variety of privacy attacks. We have evaluated our framework using a real prototype developed in Android and Hadoop HBase as well as realistic WiFi traces scaling-up to several GBs. Our analytical evaluation and experimental study reveal that TVM is not vulnerable to attacks that traditionally compromise $k$-anonymity protection and indicate that TVM can offer fine-grained localization in approximately four orders of magnitude less energy and number of messages than competitive approaches.

EXISTING SYSTEM

WiFi-based positioning systems used in existing system. GPS is unavailable in indoor spaces and consumes considerable energy.
DRAWBACK OF EXISTING SYSTEM

- Rely on server-side.
- Service provider to know the location of a user at all times

PROPOSED SYSTEM

Protecting users from location tracking by the localization service, without hindering the provisioning of fine-grained location updates on a continuous basis. Our proposed Temporal Vector Map (TVM) algorithm, allows a user to accurately localize by exploiting a k-Anonymity Bloom (kAB) filter and a bestNeighbors generator of camouflaged localization requests, both of which are shown to be resilient to a variety of privacy attacks.

ADVANTAGE OF PROPOSED SYSTEM

- TVM is not vulnerable to attacks that traditionally compromise k-anonymity protection.
- Fine-grained localization.
- Less energy for magnitude.
- Energy-efficient manner and without expensive additional hardware.
- It provide the accurate location (position) of a user.

SYSTEM SPECIFICATION

Hardware Requirements

System : Pentium IV 2.4 GHz
Hard Disk : 40 GB
Software Requirements

Operating system : Windows Family
Tools : eclipse
Technology Used : Java
Backend Used : SQLITE

Floppy Drive : 1.44 Mb
Monitor : 15 VGA Colour
Mouse : Logitech
Ram : 512 Mb