Sensitivity and Semantic Aware Protection of Location Privacy

Berker Ağır, Jean-Paul Calbimonte, Esiam Ashraf, Karl Aberer
Distributed Information Systems Laboratory (LSIR), EPFL

Location-Privacy Problem in Continuous Data Disclosure

- Everyday applications and ubiquitous devices contribute data to the Internet of Things in a continuous nature.
- Oftentimes, the data disclosed is accompanied by sensitive information such as location and time.
- Need of privacy protection mechanisms (e.g., obfuscation, hiding).

Adaptive Location-Privacy Protection

In previous work [1], it is shown that an adaptive protection approach not only protects location-privacy better, but also causes less utility loss.

Adaptive Location-Privacy Protection

- Not all the locations require the same level of protection:
  - A hospital might be sensitive for patients
  - Introducing a sensitivity profile for users that represent varying privacy requirements for varying circumstances:
    - Time of day, semantics, activity, etc.

An Android Library for Widespread Protection

- We have developed an Android library and an application that integrates this library to protect user’s location privacy considering:
  - location semantics fetched from OpenStreetMap
  - Sensitivities based on location semantics and geographical locations

References