nano-tera.ch
swiss scientific initiative in health / security / environment systems

OpenSense 2 RTD 2013

FNSNF

Sensitivity and Semantic Aware Protection of Location Privacy

Berker Ağır, Jean-Paul Calbimonte, Eslam Ashraf, Karl Aberer

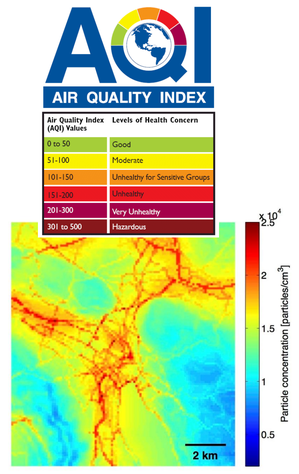
Distributed Information Systems Laboratory (LSIR), EPFL

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Human-centric Applications

Active Internet Presence → abundant data disclosure on Internet platforms (e.g. OSNs)

Human as sensor → infer context of users from mobile data and social networks



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**
  - → Assault and robbery concerns
  - → Political orientation
  - → Habits
  - → Private relations

Need of privacy protection mechanisms (e.g., obfuscation, hiding)

Most of the existing approaches to location-privacy protection

- have **static** parameters,
- do not consider **individual** concerns,
- rely on **trusted** anonymization servers,
- do not consider **smart adversaries,**
- do not take into account **trajectory history,**
- lack multidimensional analysis and protection

not enough privacy-protection due to cumulative or circumstantial exposure

no consideration of **sensitivities** and **semantics**

overprotection, thus lower data utility

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.

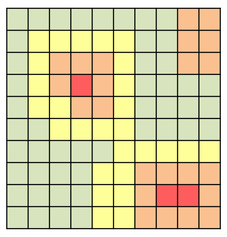
It is important to build on top of adaptive strategies to encompass additional dimensions such as **location semantics** and **user sensitivities** [2].

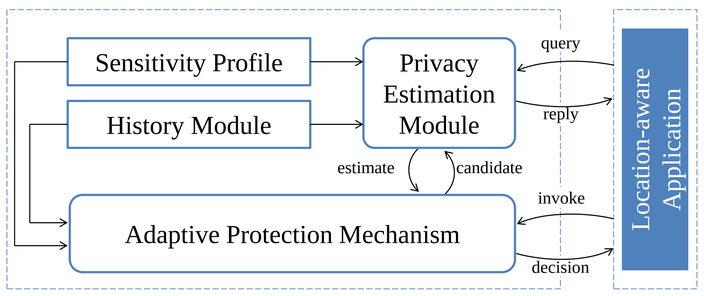
Not all the locations require the same level of protection

- 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.





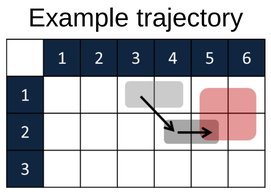
Lightweight, Bayesian updating

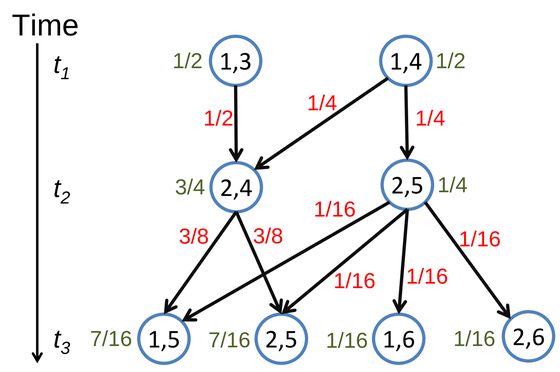
Spatial obfuscation with ***adaptive*** configuration of the cloaking area (CA) [1].

Local estimation of location privacy using **a linkability graph** utilizing the *distortion-based* metric (Expected Distortion – ED) [3].

$$ED(u,t) = \sum_{ol_t} D(\mathrm{loc}(u,t), ol_t) \cdot Pr(u, ol_t)$$

Example trajectory

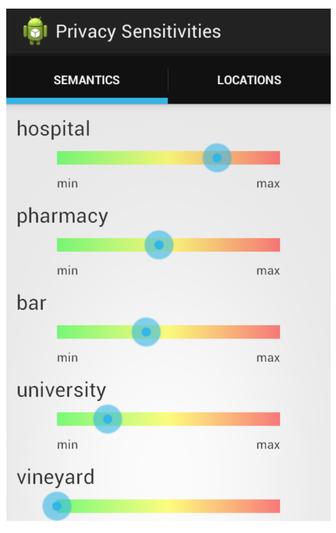




An Android Library for Widespread Protection

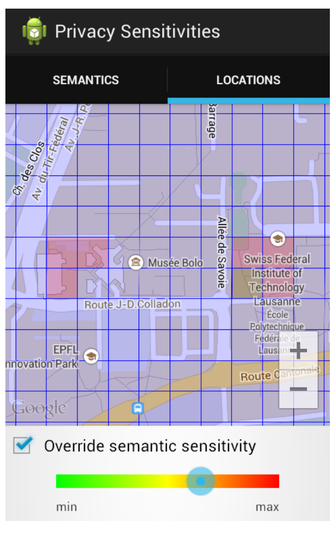
- We have developed an Android library and an application that integrates this library to protect user's location privacy considering:
  - **location semantics** fetched from OpenStreetMap
  - **Sensitivities** based on location semantics and geographical locations

Setting Screen for Privacy Sensitivities

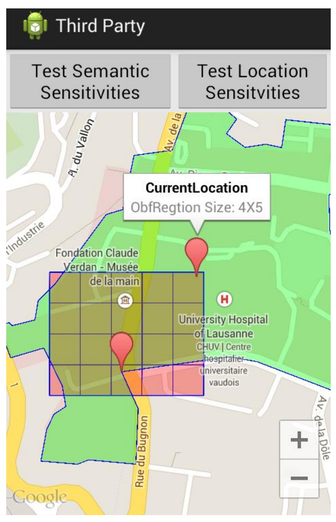


Intuitive way of setting which types of locations are sensitive for the user

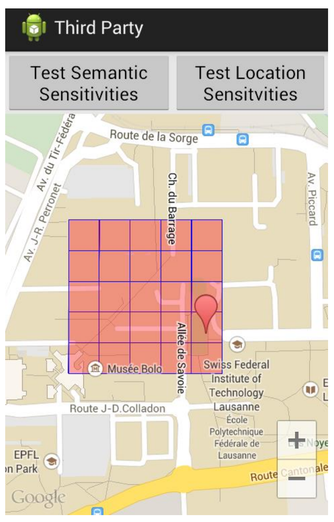
Possibility to **override** any semantic sensitivity setting for a certain region and set a localized sensitivity level



Adaptive Protection Mechanism in Action



Our adaptive protection mechanism automatically considers the sensitivity settings and generates appropriate cloaking areas for the user's location



References

[1] B. Agir, T. G. Papaioannou, R. Narendula, K. Aberer and J.-P. Hubaux. *User-side adaptive protection of location privacy in participatory sensing*, in Geoinformatica, vol. 18, num. 1, p. 165-191, 2014.

[2] B. Agir, J.-P. Calbimonte and K. Aberer. *Semantic and Sensitivity Aware Location-Privacy Protection for the Internet of Things,* Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn), 2014.

[3] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux. *A Distortion-based Metric for Location Privacy*. In ACM Workshop on Privacy in the Electronic Society (WPES), 2009.