

Protecting and Quantifying Privacy in Mobile Crowd Sensing



Berker Ağır, Jean-Paul Calbimonte, Karl Aberer, T. Papaioannou, R. Narendula, J.-P. Hubaux

Distributed Information Systems Laboratory (LSIR), EPFL

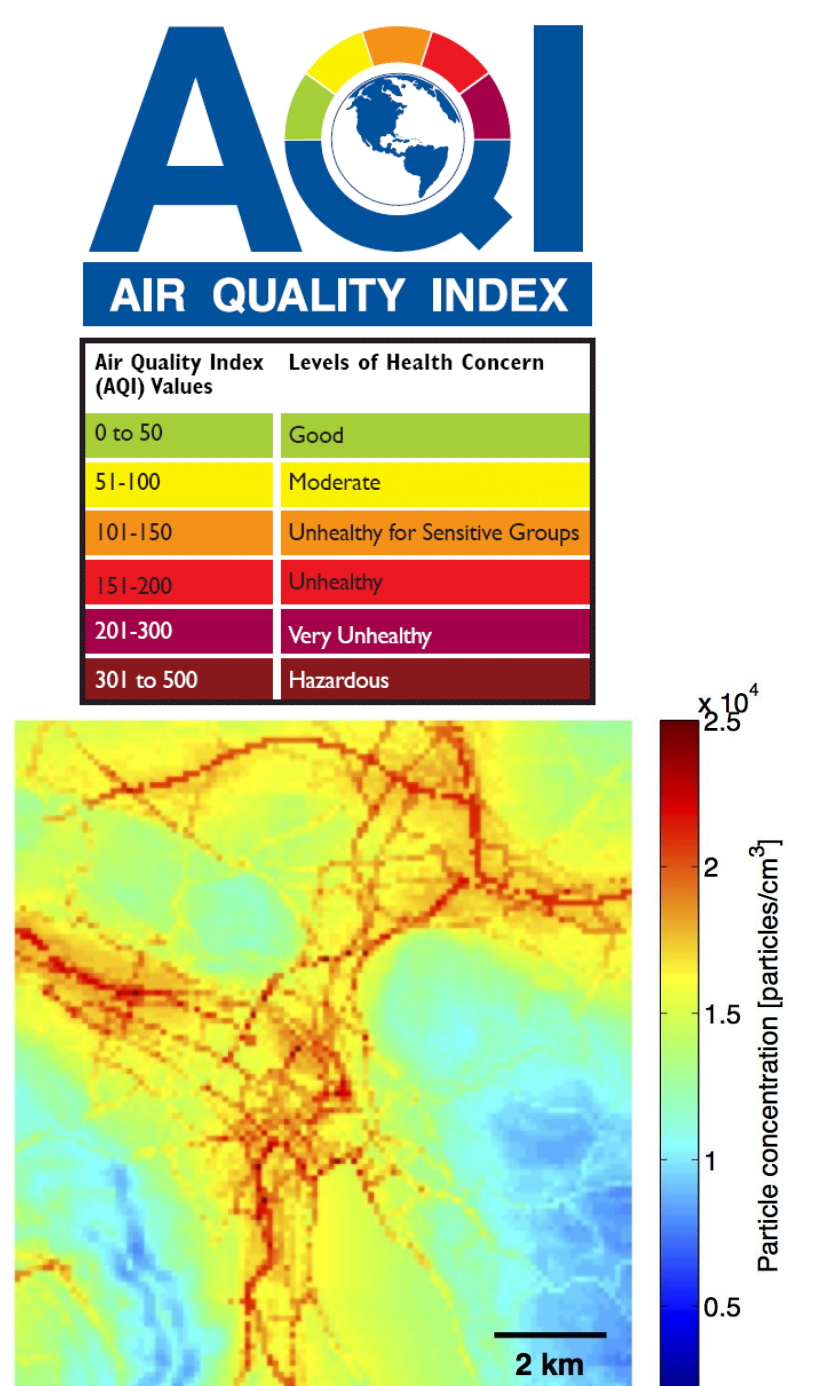
From purely **infrastructure-centric** monitoring to a **participatory setting**



Human-centric sensing



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



Location-Privacy Problem in Continuous Data Disclosure

- Crowd sensing requires *abundance* of data for ensuring high utility requiring a **continuous** data reporting scheme
- Sensed data is accompanied by **location** and **time** information
- Location information carries highly contextual data
 - Assault and robbery concerns
 - Political orientation
 - Habits
 - Private relations

Need of location-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 take into account **trajectory history**.

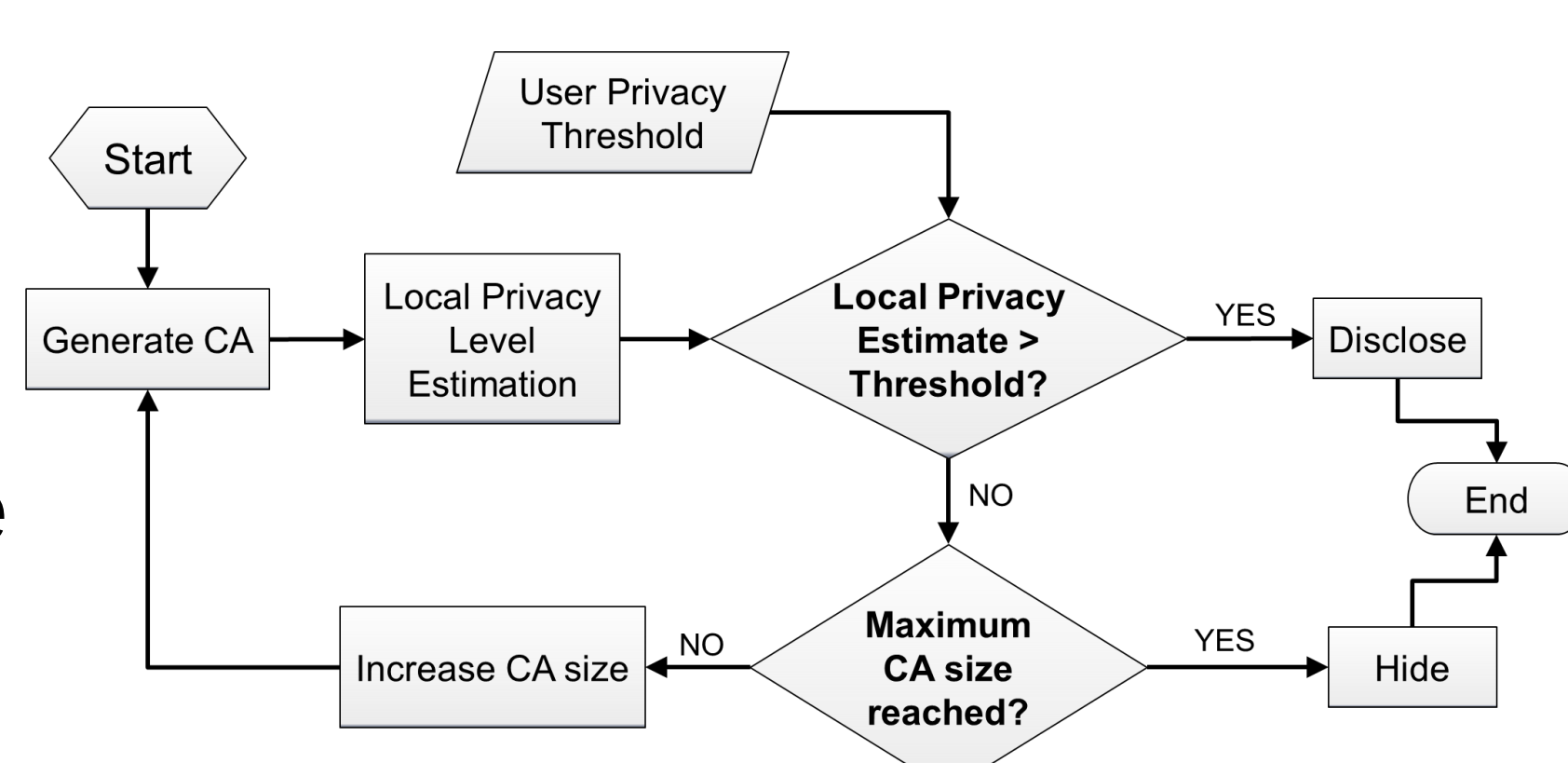
not enough privacy-protection due to cumulative or circumstantial exposure

overprotection, thus lower data utility

Adaptive Location-Privacy Protection

We employ **spatial obfuscation** and **data hiding** and **adaptively** choose the size of the cloaking area (CA) and the extend of data hiding.

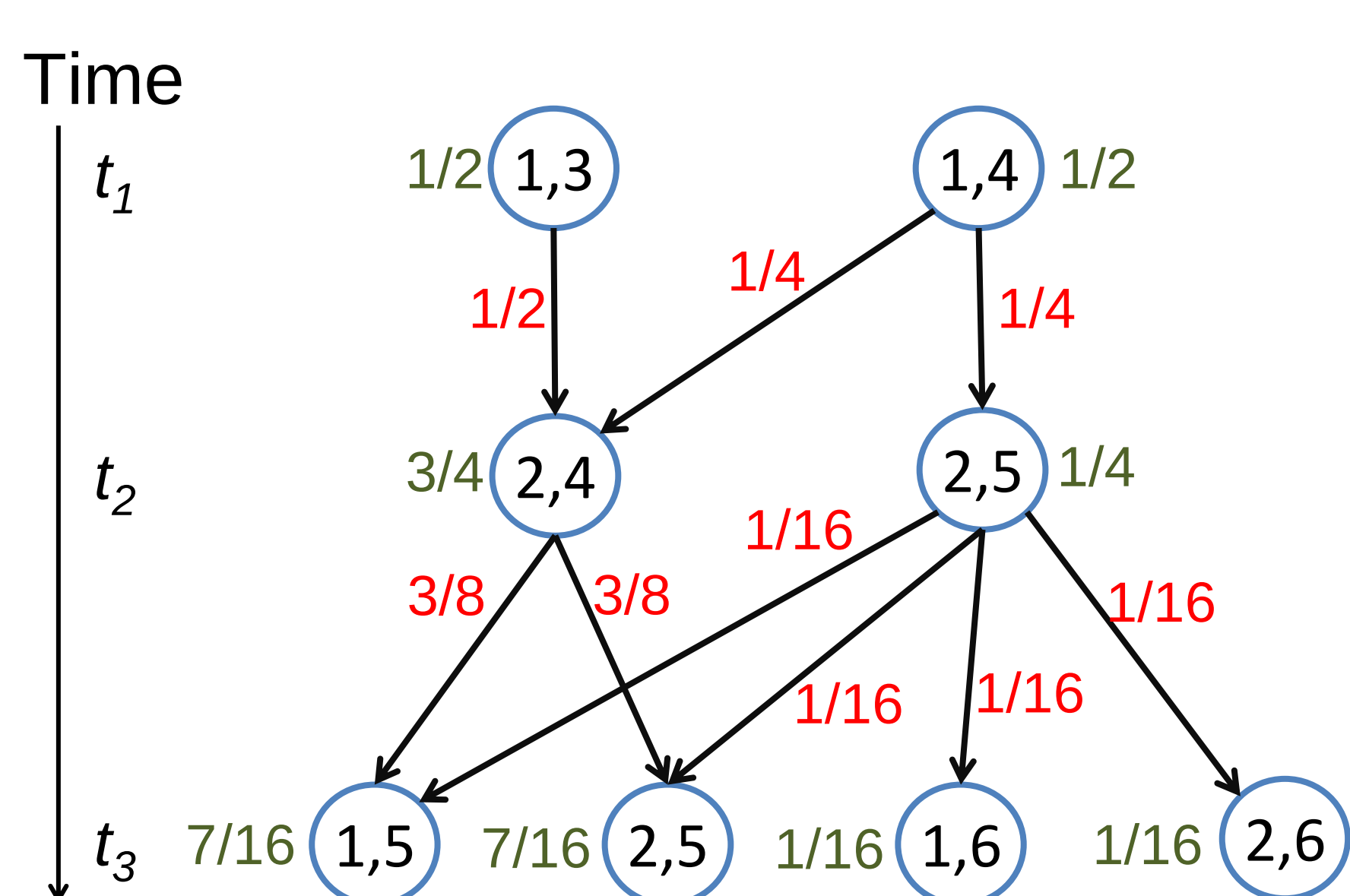
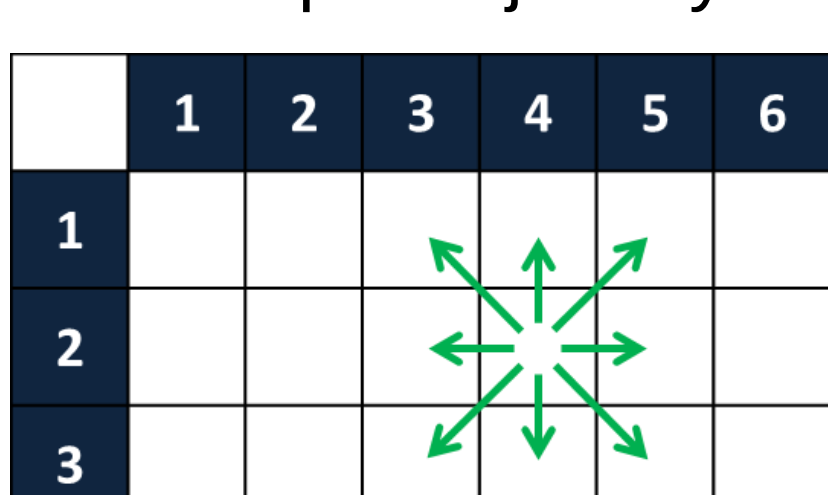
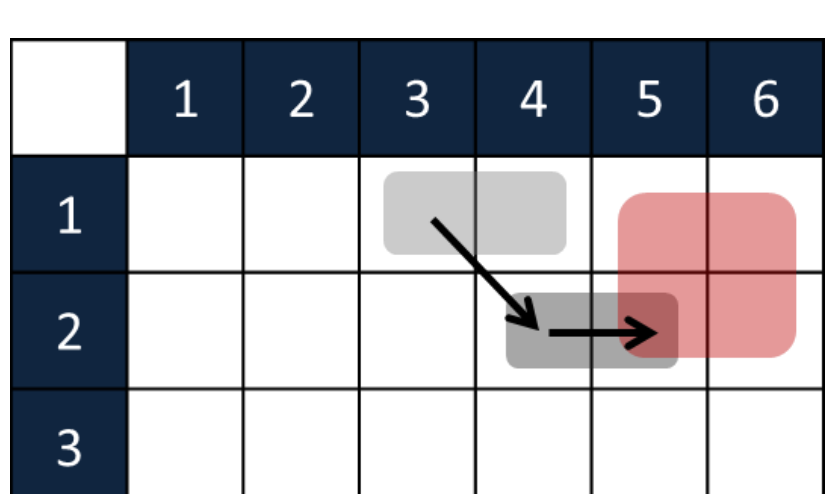
This is realized through **local** estimation of privacy-leakage using **a linkability graph** utilizing the **distortion-based** metric (Expected Distortion – ED) [3].



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

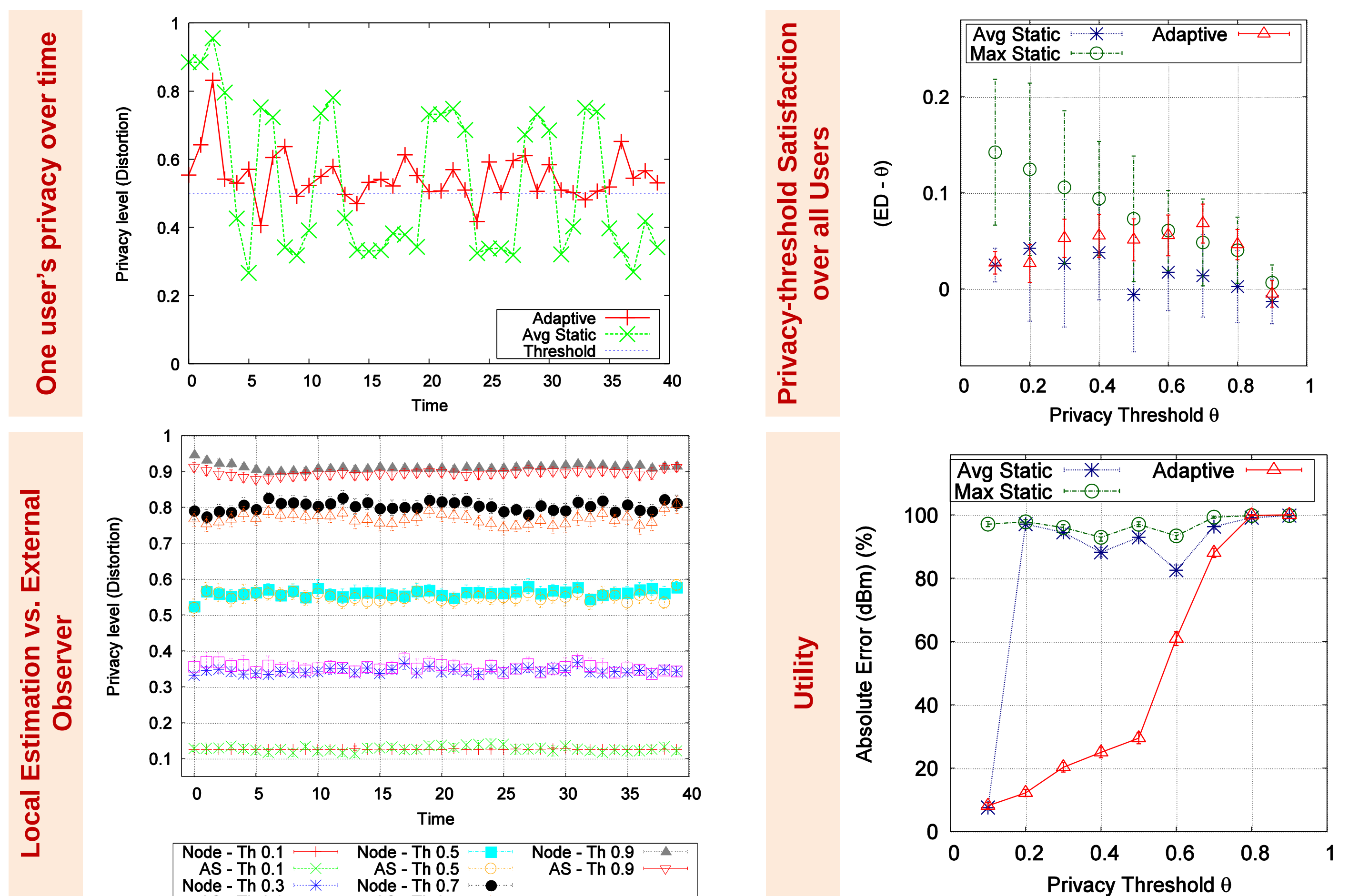
Lightweight, Bayesian updating

Linkability Graph for Privacy Estimation



Evaluation

- Electrosmog sensing scenario
- 40 real traces from the Lausanne Data Collection Campaign [2]
- Comparison to static protection approaches
- Privacy evaluation (as observed by an external observer) using the Location-Privacy Meter (LPM) [4]



It is shown that an adaptive protection approach not only protects location-privacy **better**, but also causes **less** utility loss.

Future Work: Integration of **location semantics** in the inference and protection of privacy & analyzing the **effect** of **measurement data** on privacy leakage

References

- [1] B. Agır, 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] Nokia Research Center. Lausanne Data Collection Campaign. <http://research.nokia.com/page/11367>.
- [3] R. Shokri, J. Freudiger, M. Jadhwal, and J.-P. Hubaux. *A Distortion-based Metric for Location Privacy*. In ACM Workshop on Privacy in the Electronic Society (WPES), 2009.
- [4] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux. *Quantifying Location Privacy*. In Proc. of IEEE Symposium on Security and Privacy (S&P), 2011.