Location Privacy in Practice

Sonia Ben Mokhtar

26/06/2015

Thanks to Vincent Primault…

Outline

1. Context
2. Location-based services
3. Threats
4. Challenges
5. Anonymization techniques
6. Sum up

Who am I?

- CNRS researcher, LIRIS lab, DRIM group
- Research topics:
  - Distributed and/or Mobile systems
    - Fault Tolerance
    - Privacy
- Coordinator of the **Priva'Mov** project funded by the **IMU** Labex.

CONTEXT: IMU PRIVA'MOV

Crowdsensing—>Smart Cities

- A novel type of **sensor networks** using the sensing capabilities of **our** handheld **devices**
  - **Personal sensing**
    - Health applications
    - Carbon footprint
  - **Community sensing**
    - Congestion monitoring
    - Air pollution monitoring

Objectives

- Crowdsensing platform
  - 100 users equipped with smartphones
  - 3 usecases (social sciences, mobile systems, transports)
- **Location privacy**

Location privacy: A state of the art

LOCATION-BASED SERVICES (LBS)

Use location to provide services

foursquare

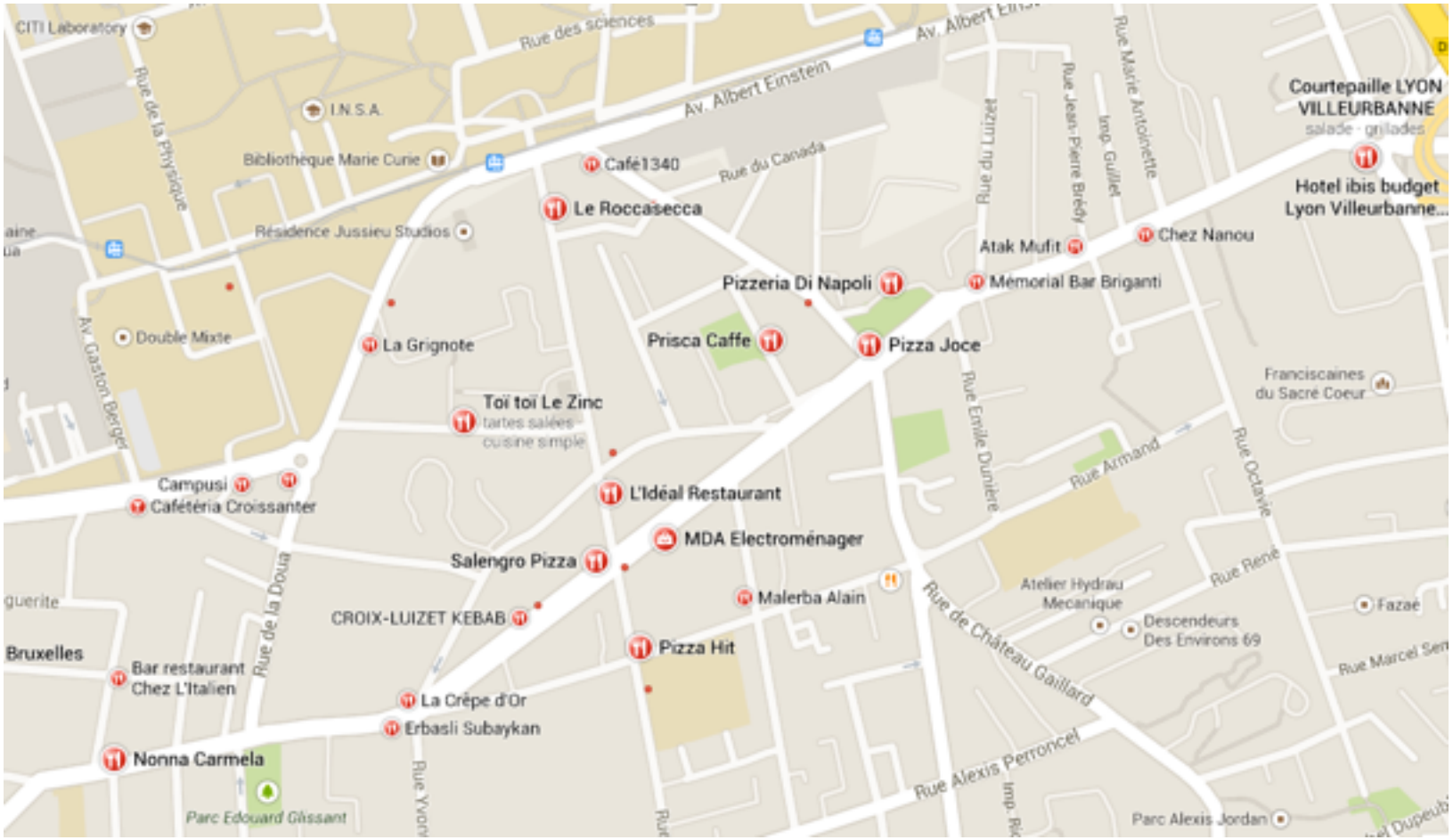
Google maps

bing™ maps

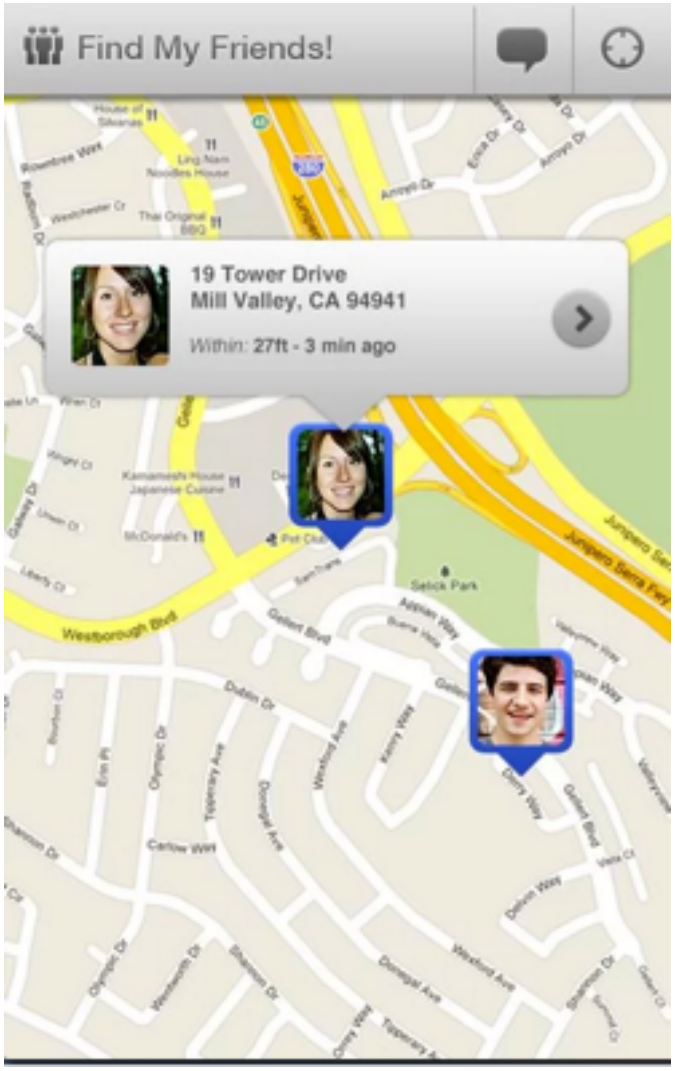
OpenStreetMap

What’s the weather like?

Find POIs around



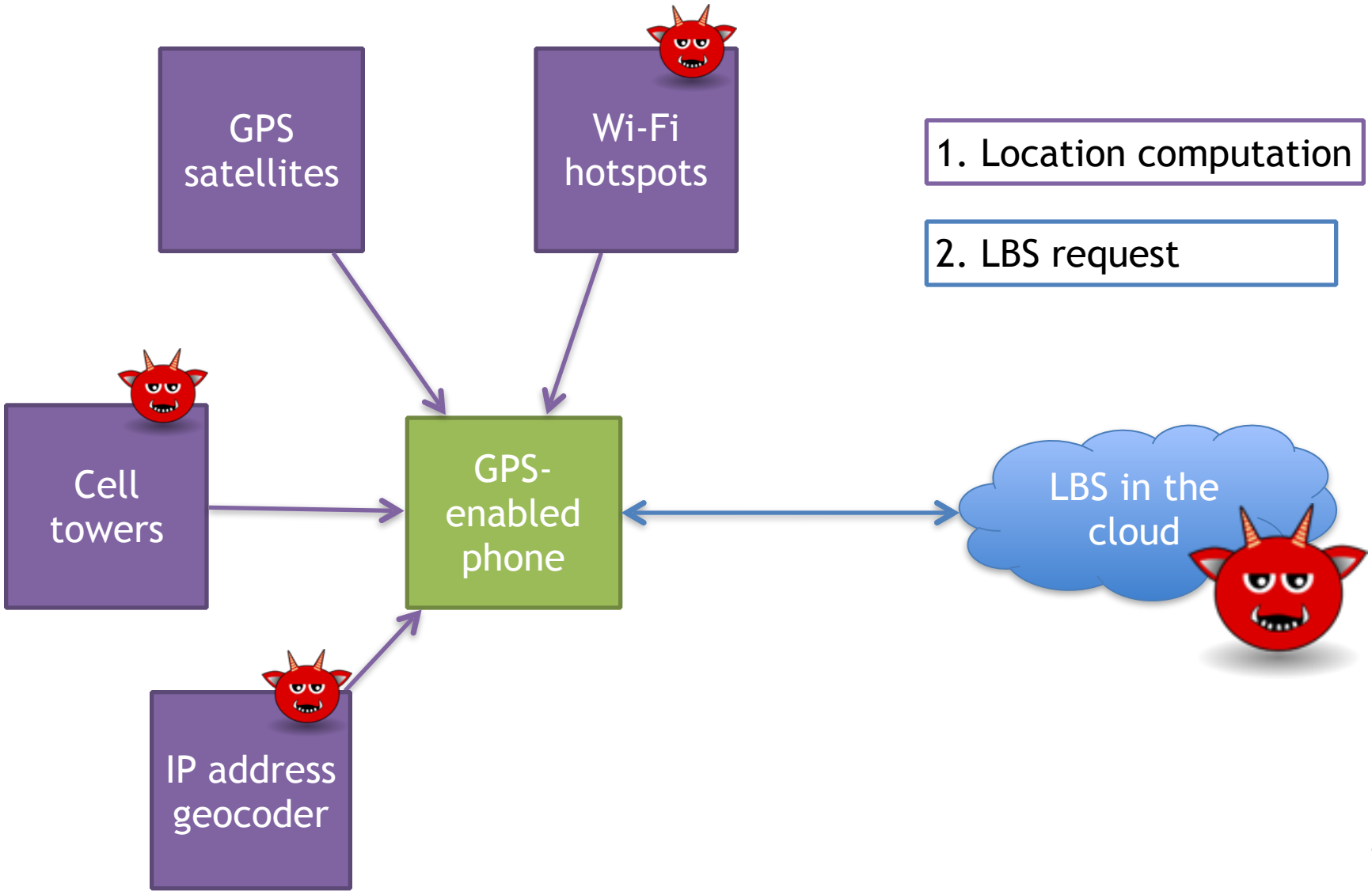
Locate nearby friends



Navigate to a destination

Play social games

Location lifecycle

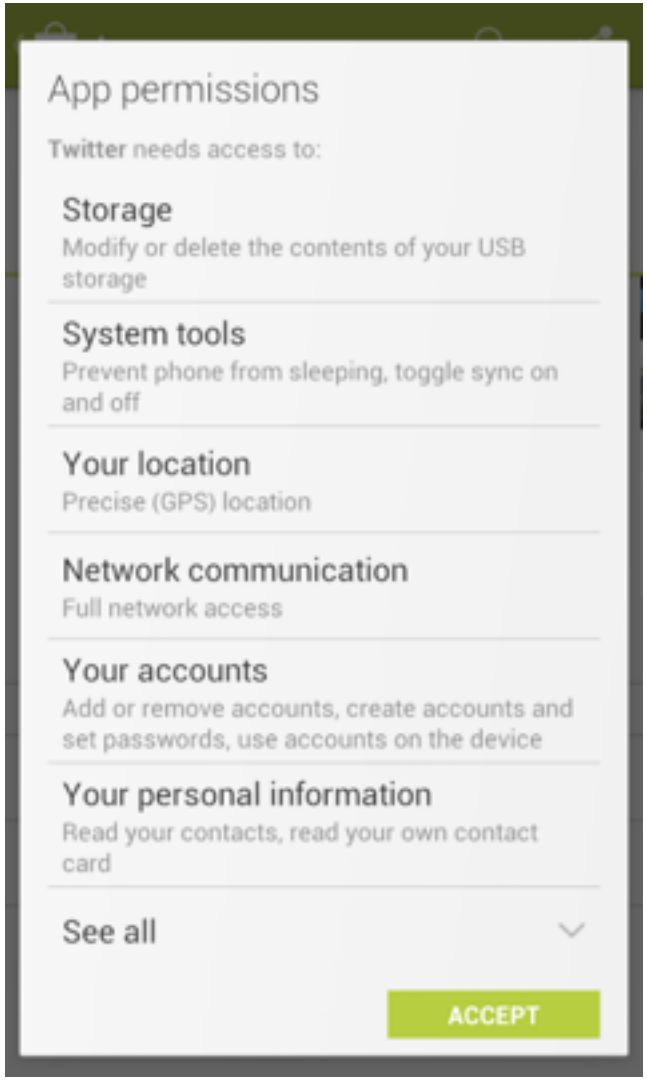


Some numbers…

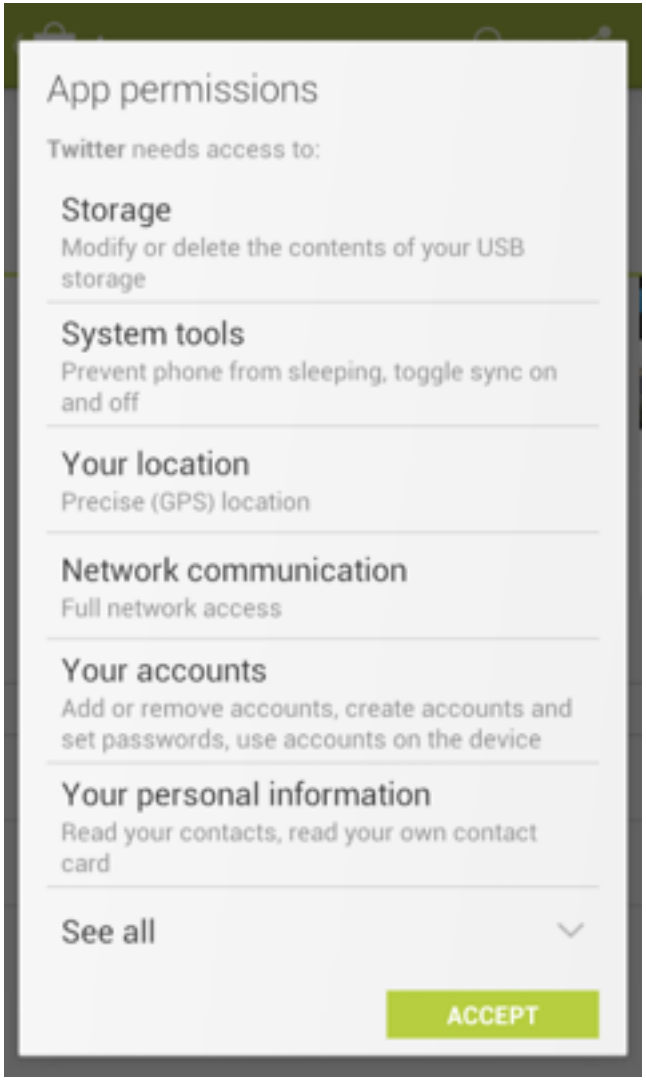
- Companies (e.g., Apple, TomTom…) have agreements to **share** location data with « partners and licensees »
- Skyhook wireless is **resolving** 400M user's WiFi locations/day
- 25B copies of applications available on the AppStore **access location data**
- ~50% of all iOS and Android traffic is available to ad networks

De Montjoye, Y.-A., Hidalgo, C., Verleysen, M. and Blondel, V. Unique in the Crowd: The privacy bounds of human mobility. Scientific reports,Scientific Reports 3, Article number: 1376, 2013.

In practice…


App permissions
Twitter needs access to:
Storage
Modify or delete the contents of your USB storage
System tools
Prevent phone from sleeping, toggle sync on and off
Your location
Precise (GPS) location
Network communication
Full network access
Your accounts
Add or remove accounts, create accounts and set passwords, use accounts on the device
Your personal information
Read your contacts, read your own contact card
See all
ACCEPT

In practice…


App permissions
Twitter needs access to:
Storage
Modify or delete the contents of your USB storage
System tools
Prevent phone from sleeping, toggle sync on and off
Your location
Precise (GPS) location
Network communication
Full network access
Your accounts
Add or remove accounts, create accounts and set passwords, use accounts on the device
Your personal information
Read your contacts, read your own contact card
See all
ACCEPT


LED LENSER P14

Location privacy: A state of the art

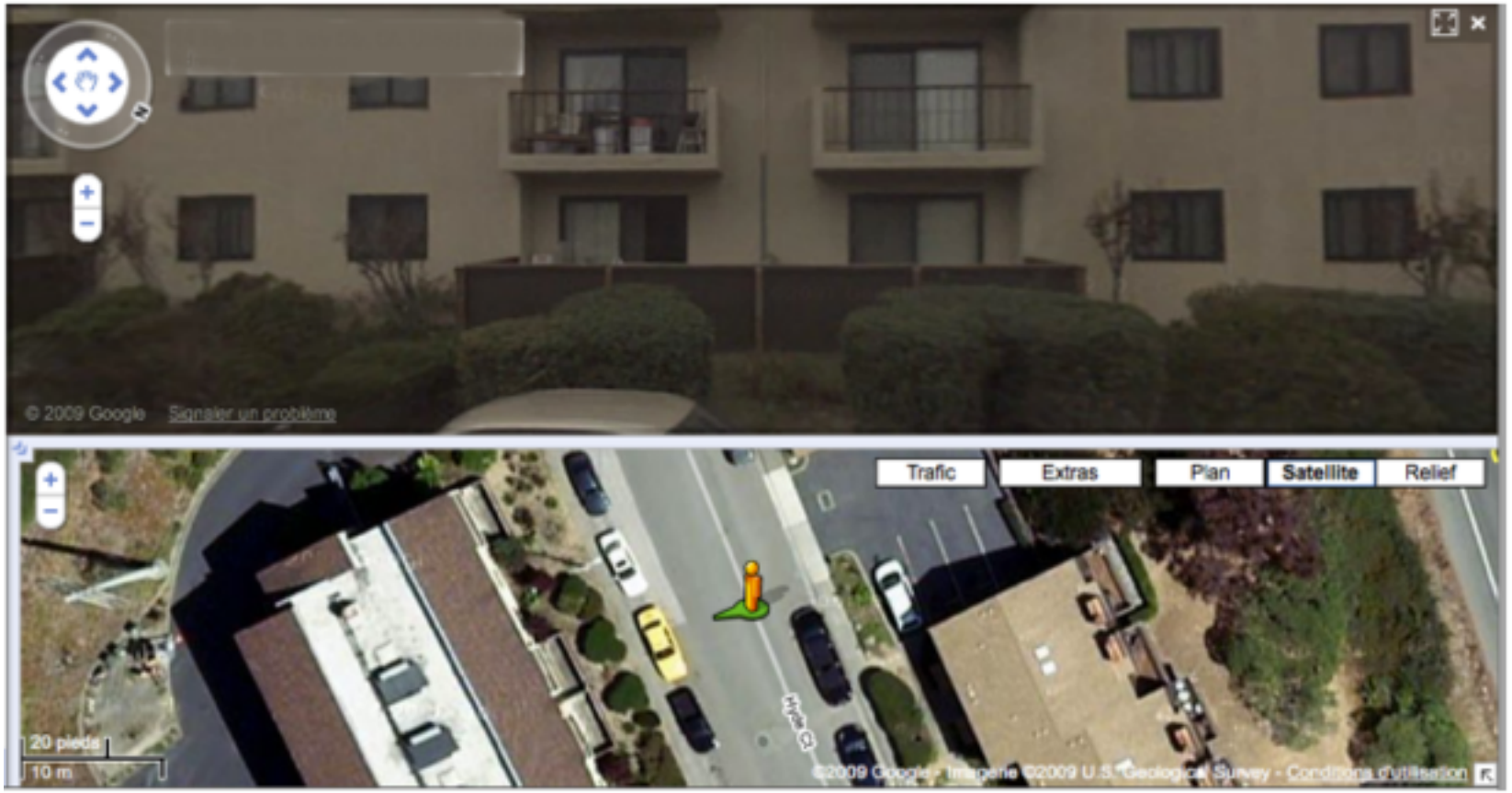
WHAT ARE THE THREATS?

PLEASE ROB ME

Raising awareness about over-sharing

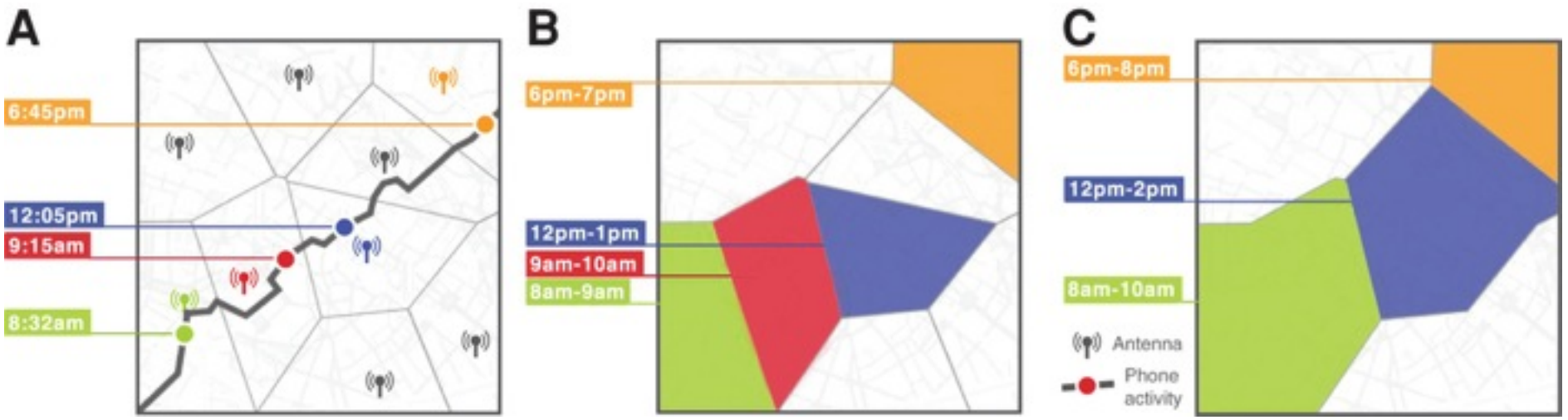
Check out our guest blog post on the CDT website.

Identifying POIs [1,2,3]



[1] Krumm, J. Inference attacks on location tracks. In Pervasive'07.
[2] Gambs, S., Killijian, M.-O. and Cortez, M. Show Me How You Move and I Will Tell You Who You Are. Transactions on Data Privacy.
[3] Golle, P. and Partridge, K. On the Anonymity of Home/Work Location Pairs. In Pervasive'09.

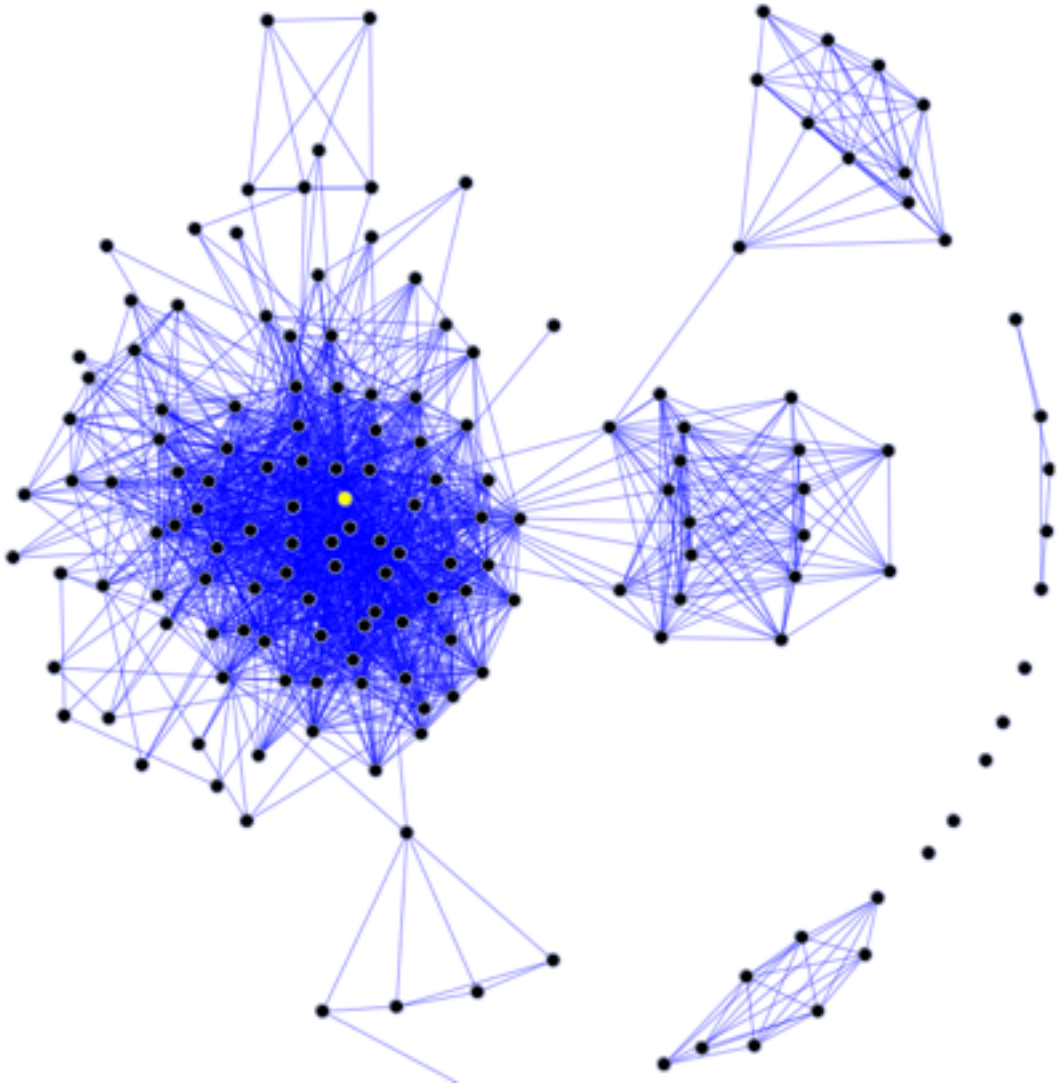
Re-identifying mobility traces [1,2]



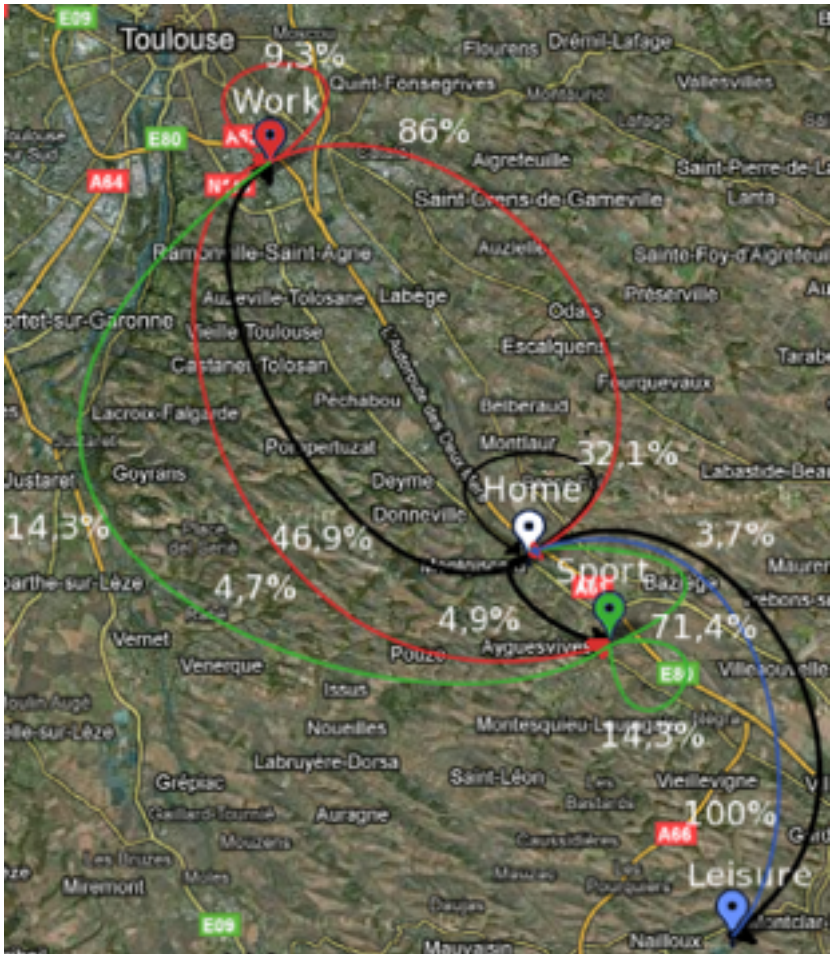
Only 4 (coarse grain) points are sufficient to uniquely identify a majority of users! [4]

[4] De Montjoye, Y.-A., Hidalgo, C., Verleysen, M. and Blondel, V. Unique in the Crowd: The privacy bounds of human mobility. Scientific reports.

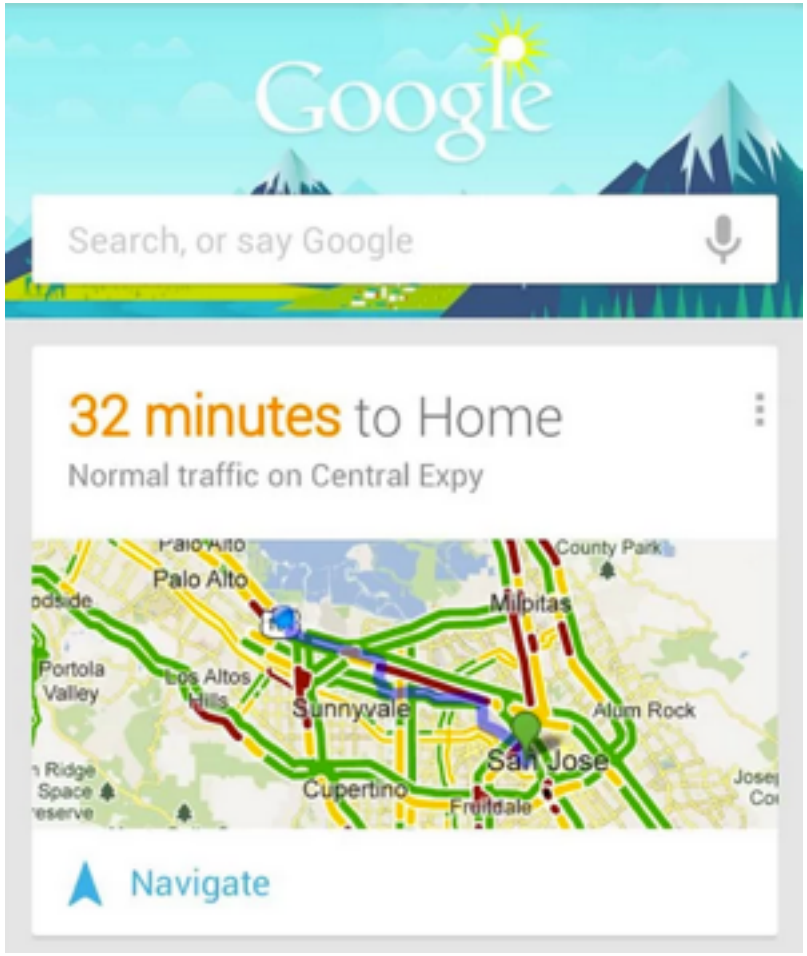
Finding out social relationships



Learning about mobility patterns [2]



Google Now already do this!



WHAT CHALLENGES ARE WE FACING?

How to query LBSs in a privacy-preserving way?

Some properties to guarantee

Privacy

Accuracy

Performance

Integration

Location privacy: A state of the art

ANONYMIZATION TECHNIQUES

Anonymization techniques

- Spatial cloaking
- Dummies
- Perturbation
- Pseudonymization
- Cryptography
- Data partitioning

Anonymization techniques

Spatial cloaking

Dummies

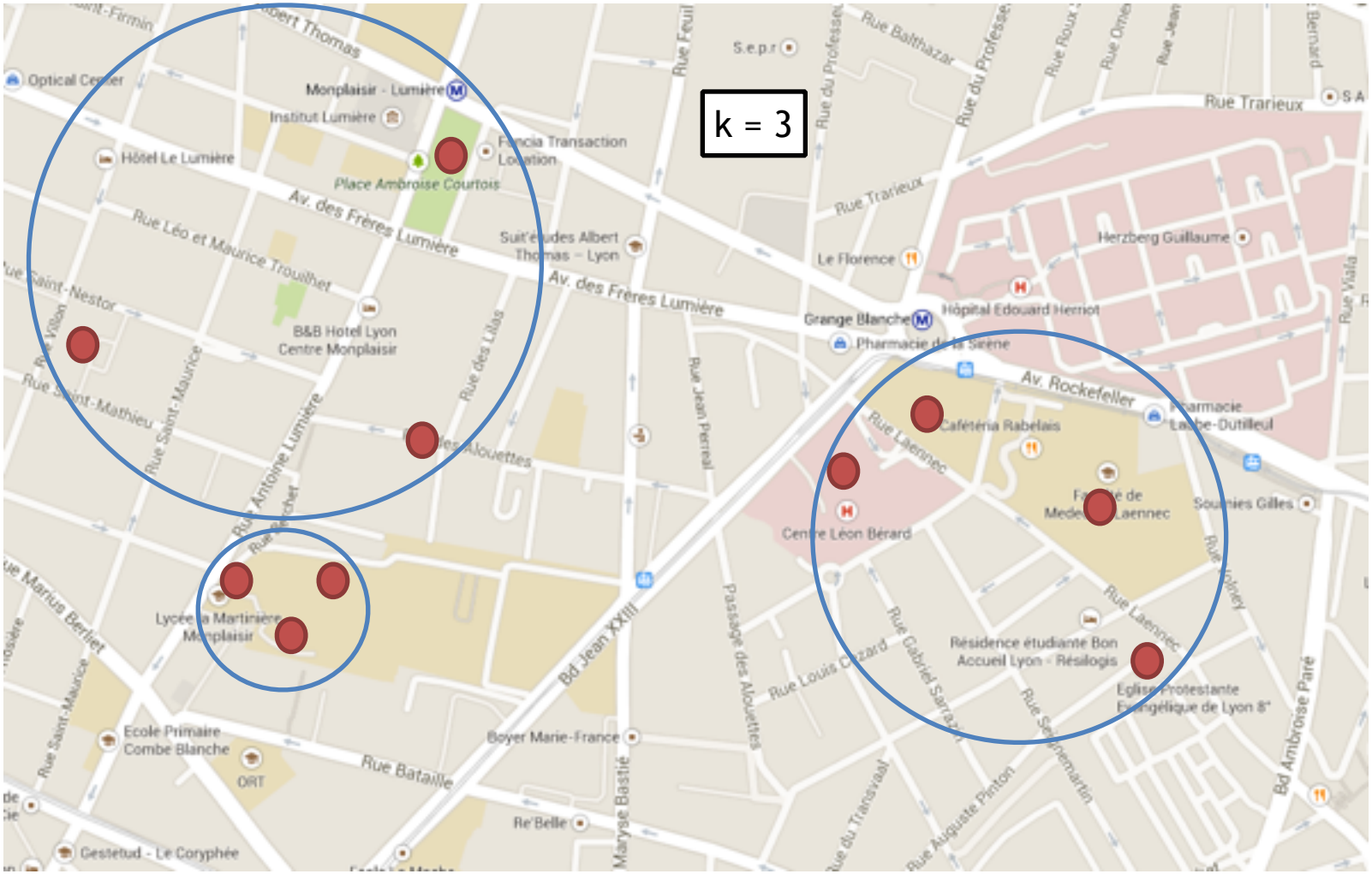
Perturbation

Pseudonymization

Cryptography

Data partitioning

Spatial cloaking [6]



[6] Gruteser, M. and Grunwald, D. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In MobiSys'03.

Drawbacks of spatial cloaking

- Attacks:
  - 2 properties to guarantee: query anonymity & location privacy [8]

- Limitations:
  - Number and density of users
  - The space often needs to be bounded and then discretized
  - Need of a trusted third party in centralized algorithms

[8] Shokri, R., Troncoso, C., & Diaz, C. Unraveling an old cloak: k-anonymity for location privacy. In WPES'10.

Anonymization techniques

Spatial cloaking

Dummies

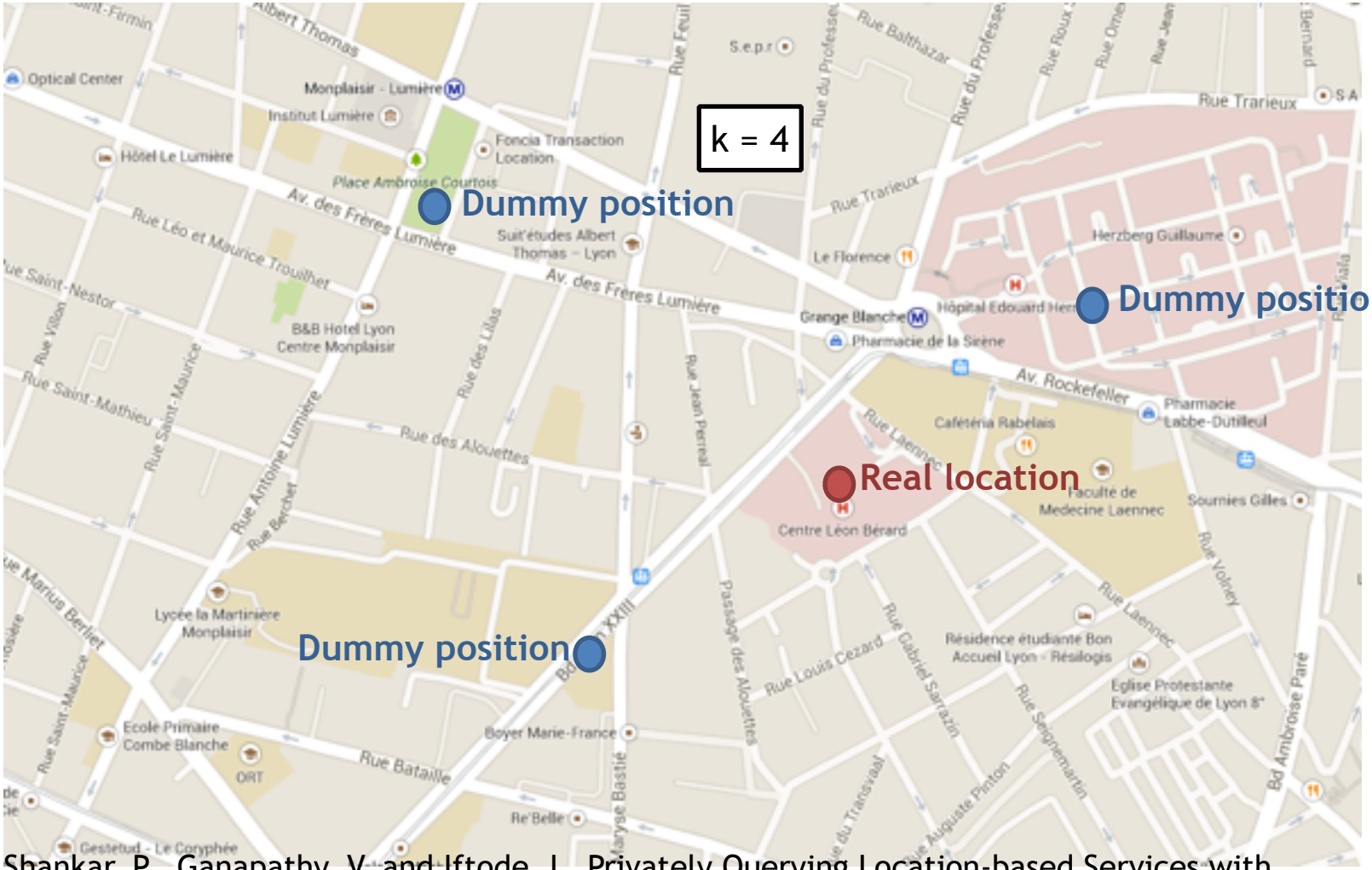
Perturbation

Pseudonymization

Cryptography

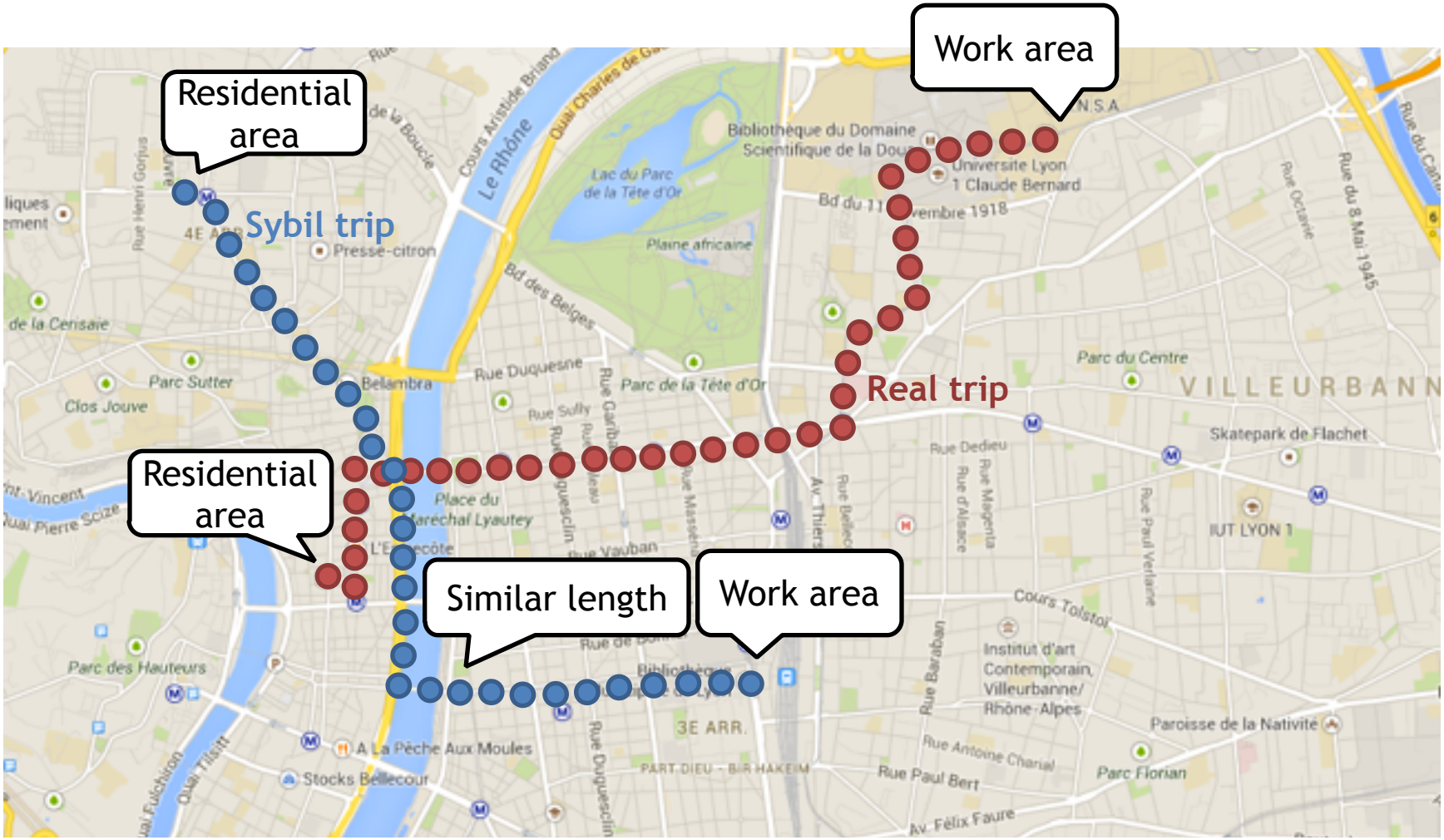
Data partitioning

Dummies [12,13]



[13] Shankar, P., Ganapathy, V. and Iftode, L. Privately Querying Location-based Services with SybilQuery. In Ubicomp'09.
[12] Kido, H., Yanagisawa, Y. and Satoh, T. Protection of Location Privacy using Dummies for Location-based Services. In ICDE'05 Workshops.

SybilQuery trips [13]



Drawbacks of dummies

- Attacks:
  - Realistic behavior of dummies
  - Data sent to the LBS contains the real position
  - Machine learning attacks reidentify real trips from those generated by SybilQuery with a probability of **93 %** [14]

- Limitations:
  - The need of external knowledge to generate realistic dummies…
  - Where to find it?
  - How to process it with limited resources?

[14] Peddinti, S. T., & Saxena, N. On the limitations of query obfuscation techniques for location privacy. In UbiComp'11.

Anonymization techniques

Spatial cloaking

Dummies

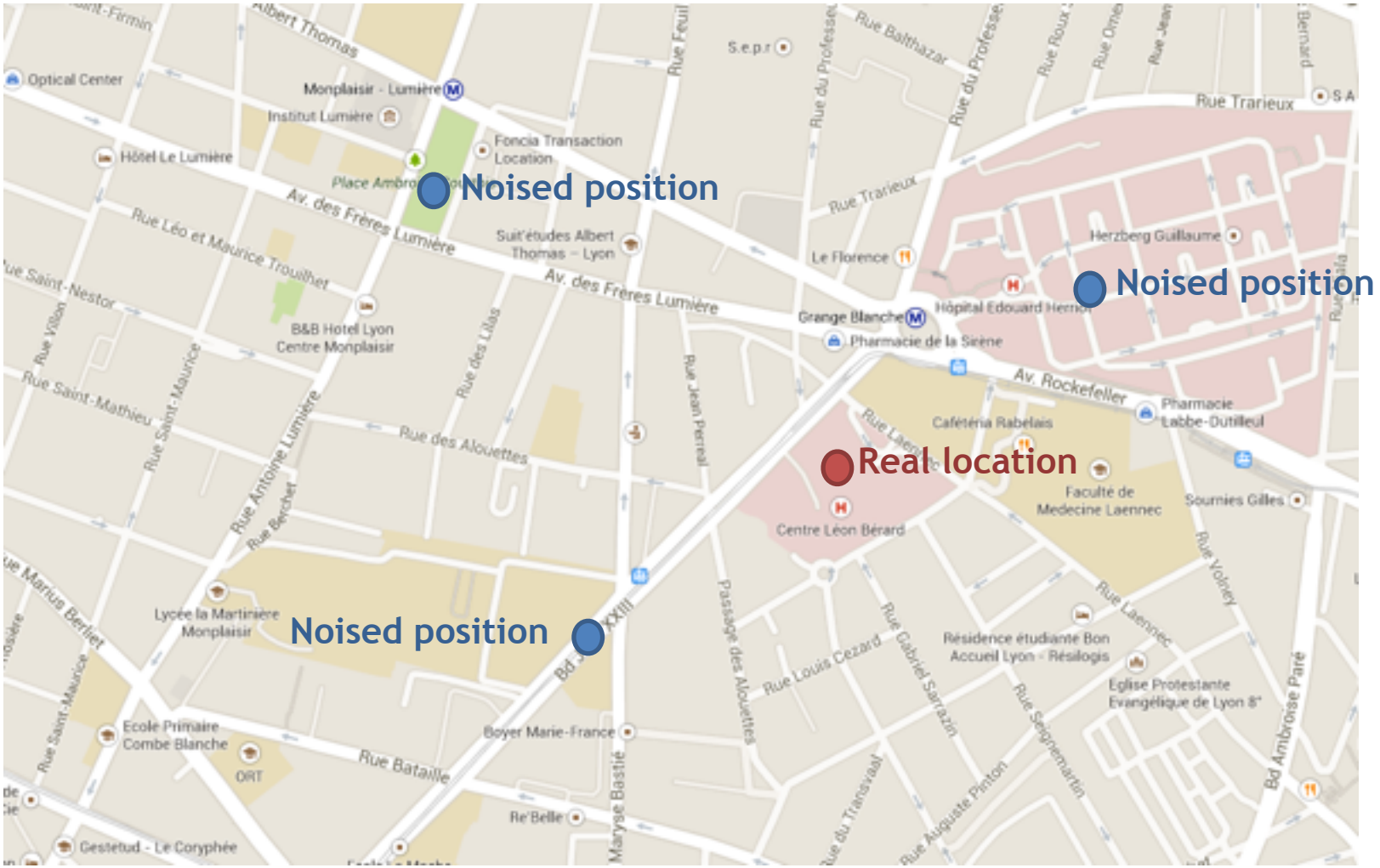
Perturbation

Pseudonymization

Cryptography

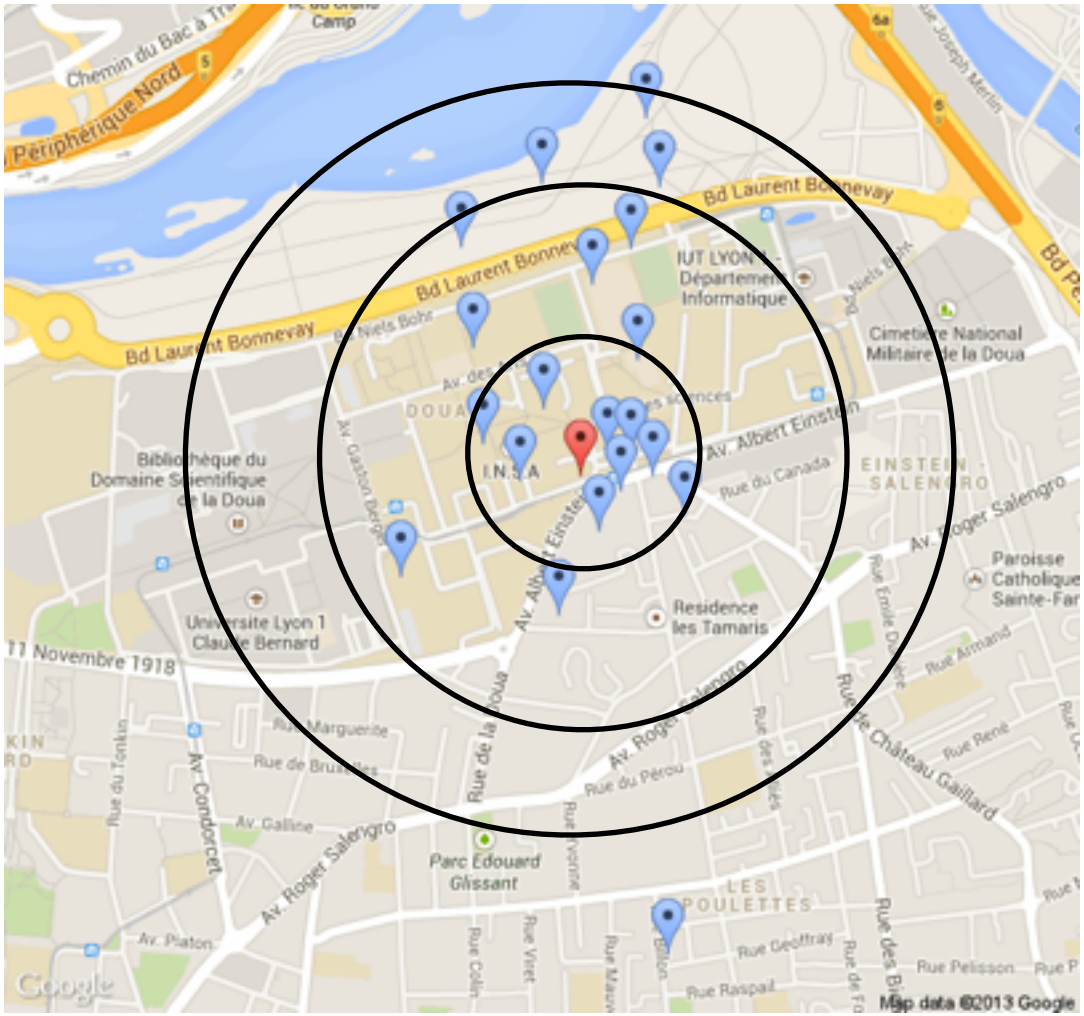
Data partitioning

Location perturbation



Geo-indistinguishable locations [16]

« The closer two points are the more indistinguishable they should be »



[16] Andrés, M., Bordenabe, N., Chatzikokolakis, K. and Palamidessi, C. Geo-Indistinguishability: Differential Privacy for Location-Based Systems. In CCS'13.

Geo-indistinguishability in practice

Differentially Private Location Privacy in Practice.V. Primault, et . al, MOST[14]

Drawbacks of location perturbation

- Attacks:
  - Clustering attacks
  - Privacy guarantees decrease when protecting multiple locations (i.e. a trace)
- Limitations:
  - Applications like navigation are complicated to implement

Anonymization techniques

Spatial cloaking

Dummies

Perturbation

Pseudonymization

Cryptography

Data partitioning

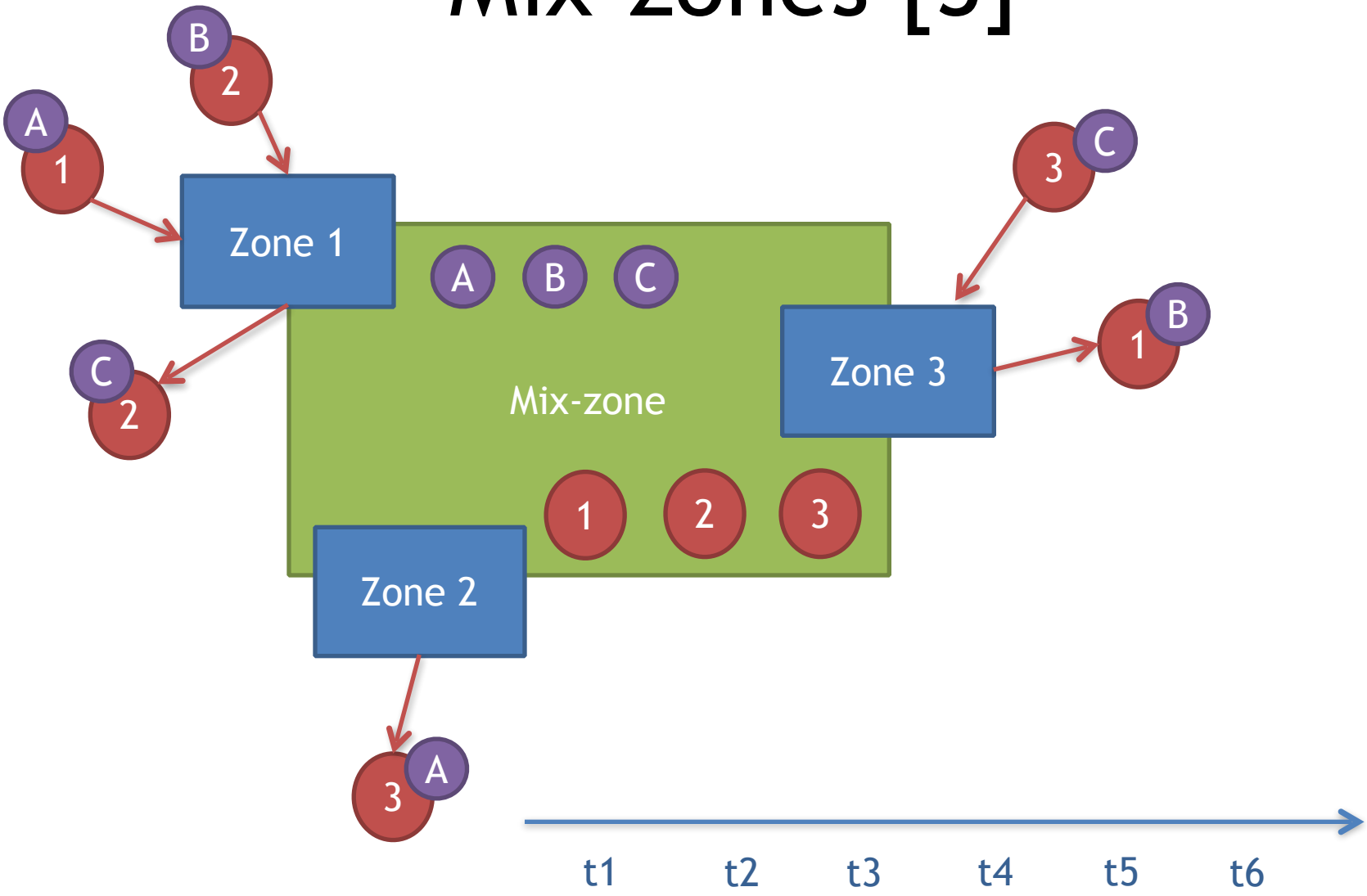
Pseudonymization

Who	Date	Latitude	Longitude
Philippe R.	*04/10/13*	*45.7829609*	*4.8750313*
Jean V.	*04/10/13*	*48.8582285*	*2.2943877*
Anne M.	*04/10/13*	*45.7783975*	*4.8794162*
Anne M.	*04/10/13*	*45.7783975*	*4.8794162*
Jean V.	*04/10/13*	*48.9545237*	*2.2012417*
Lucie E.	*04/10/13*	*45.7671436*	*4.8329685*
Jean V.	*04/10/13*	*48.9545237*	*2.2012417*
Philippe R.	*04/10/13*	*45.7829945*	*4.8960415*
Anne M.	*04/10/13*	*45.7783975*	*4.8794162*
Philippe R.	*04/10/13*	*45.8034791*	*4.9713056*
Jean V.	*04/10/13*	*51.6640214*	*3.1027893*

Pseudonymization

Who	Date	Latitude	Longitude
A	*04/10/13*	*45.7829609*	*4.8750313*
B	*04/10/13*	*48.8582285*	*2.2943877*
C	*04/10/13*	*45.7783975*	*4.8794162*
C	*04/10/13*	*45.7783975*	*4.8794162*
B	*04/10/13*	*48.9545237*	*2.2012417*
D	*04/10/13*	*45.7671436*	*4.8329685*
B	*04/10/13*	*48.9545237*	*2.2012417*
A	*04/10/13*	*45.7829945*	*4.8960415*
C	*04/10/13*	*45.7783975*	*4.8794162*
A	*04/10/13*	*45.8034791*	*4.9713056*
B	*04/10/13*	*51.6640214*	*3.1027893*

Mix-zones [5]



[5] Beresford, A. and Stajano, F. Location Privacy in pervasive computing. Pervasive Computing, IEEE.

Drawbacks of mix-zones

- Attacks:
  - Re-identification by using physical/logical laws
- Limitations:
  - Number and density of users
  - *k* is hard to enforce in practical use
  - Need of a central pseudonym server
  - Placement of mix-zones

Anonymization techniques

Spatial cloaking

Dummies

Perturbation

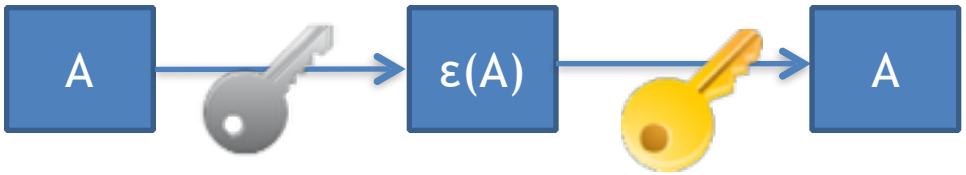
Pseudonymization

Cryptography

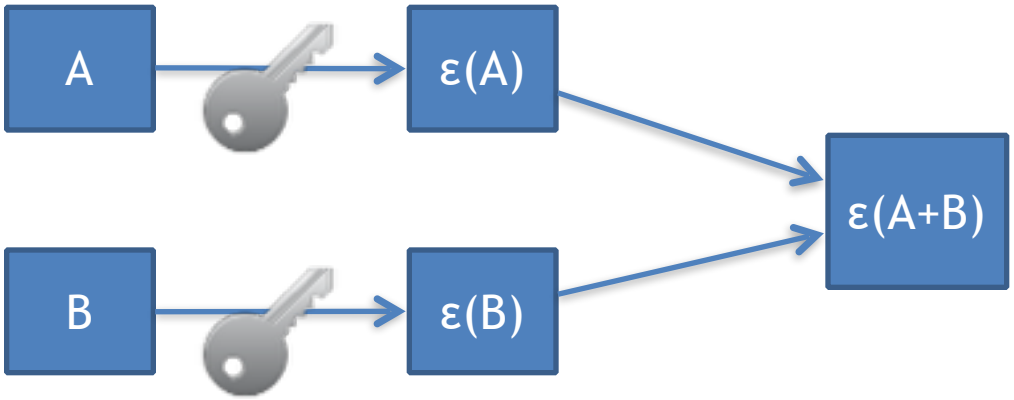
Data partitioning

Cryptographic protocols

Symmetric and asymmetric encryption



Homomorphic encryption



Drawbacks of cryptographic protocols

- Attacks:
  - Security depends on the underlying cryptographic techniques used
- Limitations:
  - Each is designed for a unique use case
  - Don’t scale well

Anonymization techniques

Spatial cloaking

Dummies

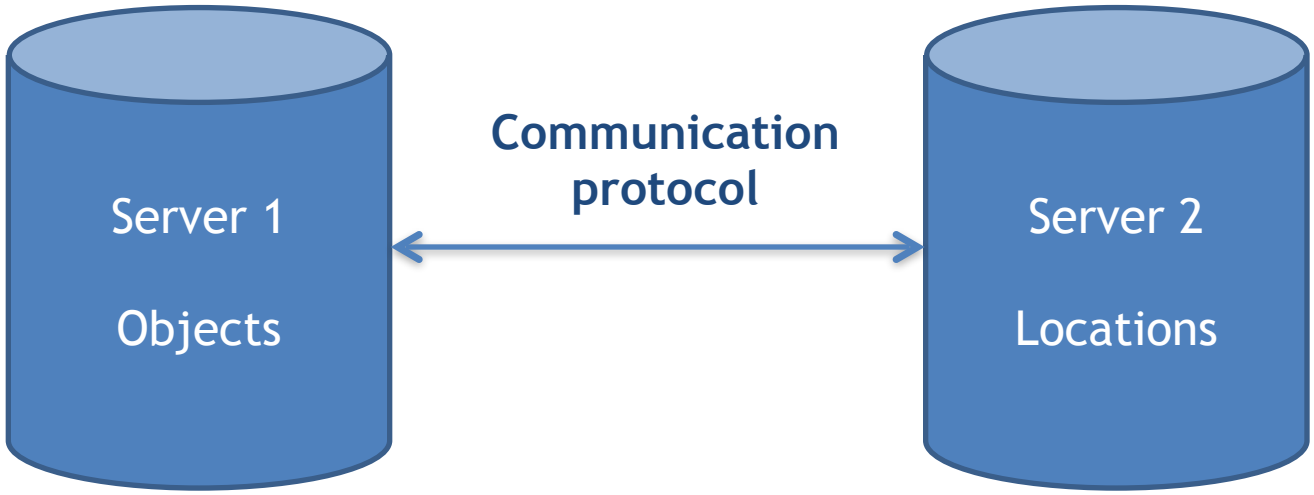
Perturbation

Pseudonymization

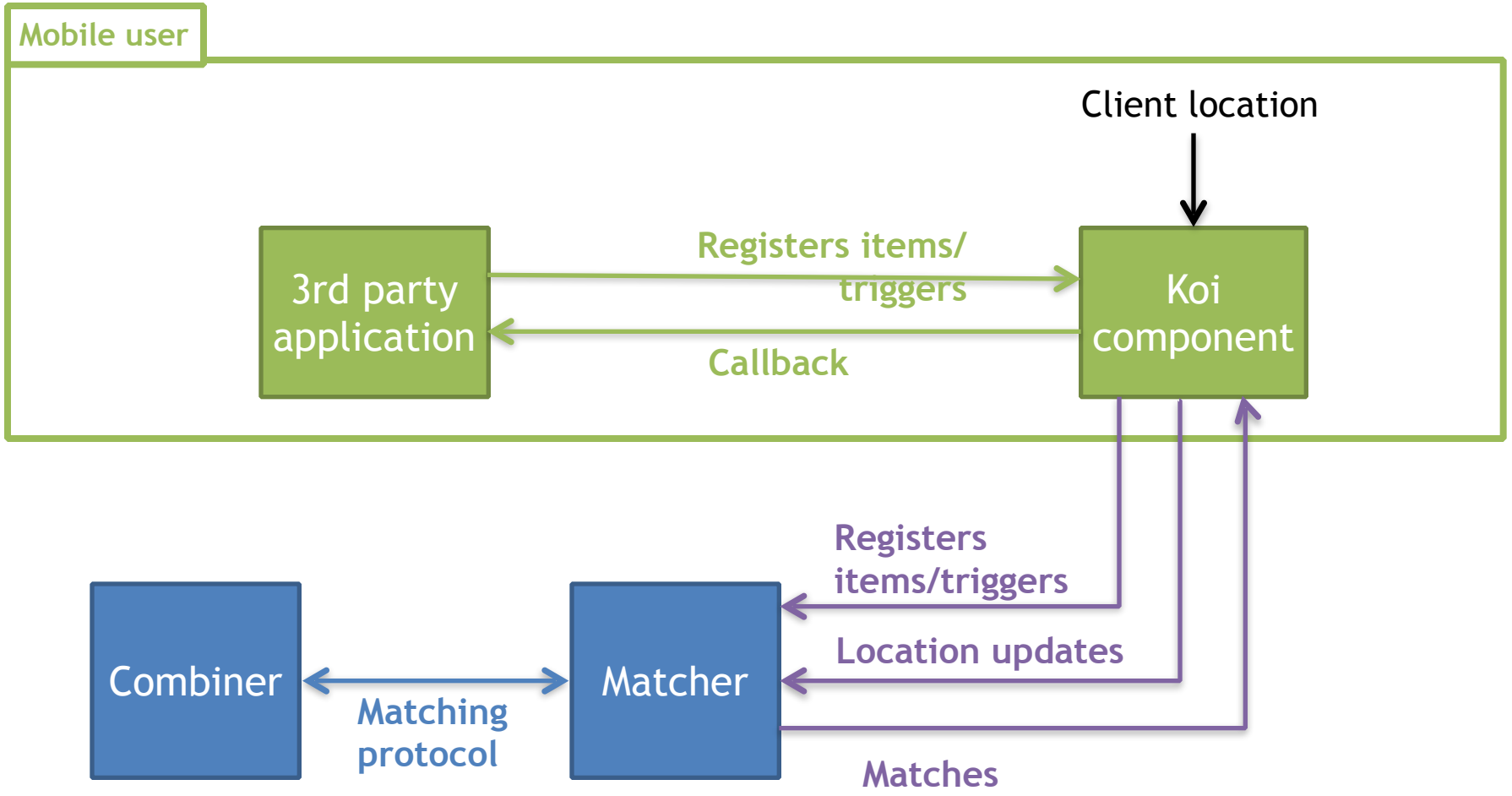
Cryptography

Data partitioning

Data partitioning



Koi architecture [23]



[23] Guha, S., Jain, M., & Padmanabhan, V. Koi: A Location-Privacy Platform for Smartphone Apps. In NSDI'12.

Drawbacks of data partitioning

- Attacks:
  - Sensibility to traffic analysis
  - Link location updates together and re-identity user
- Limitations:
  - Non-colluding servers
  - Needs to rebuild a database of POIs

Location privacy: A state of the art

SUM UP

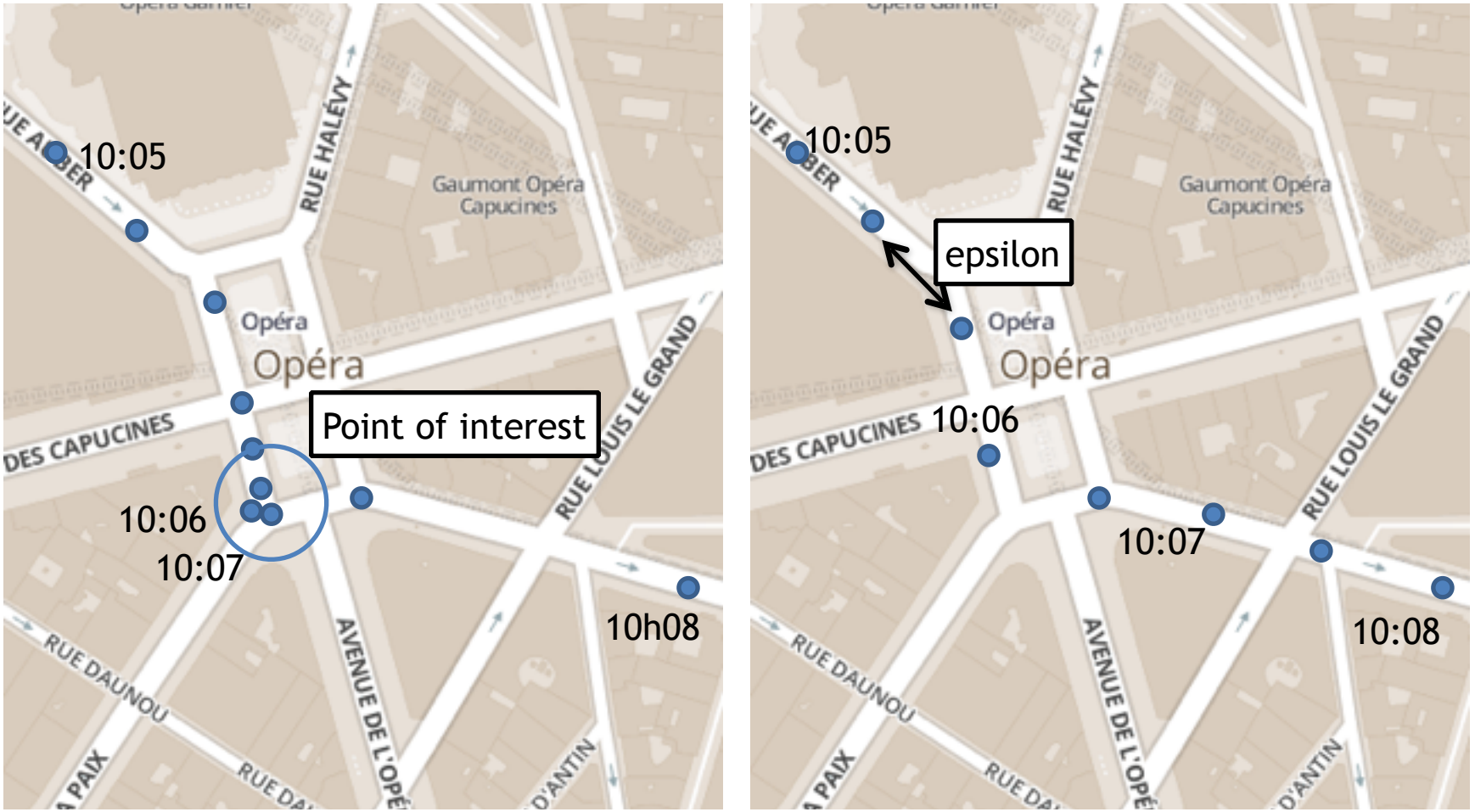
Conclusions and Future Directions

- Location data is sensitive!
- Existing solutions:
  - Are vulnerable to re-identification attacks
  - **Spatial obfuscation** alters location information

—> New protection mechanism for data publishing, that minimally distorts location

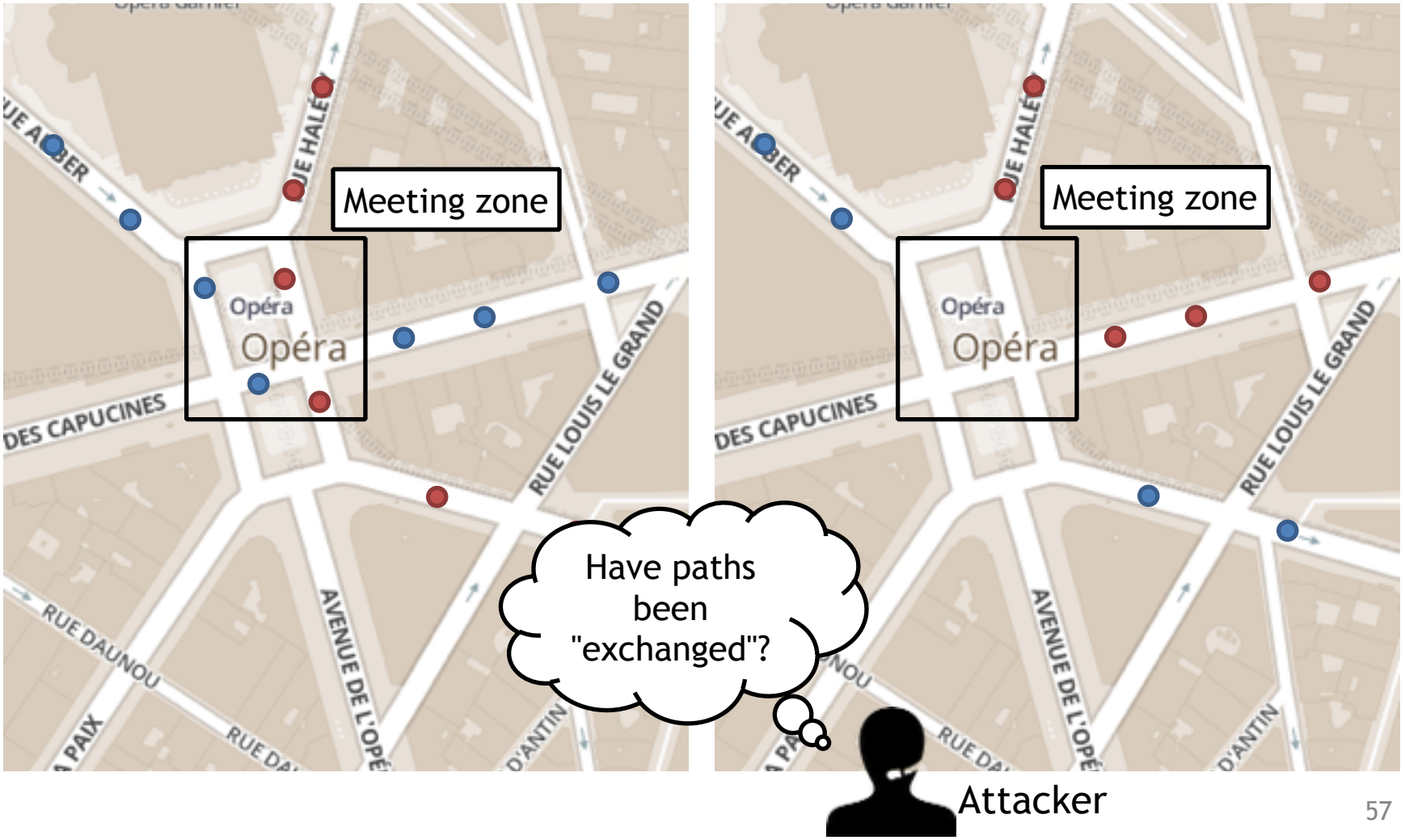
—> Towards **temporal obfuscation**

Future Directions: Speed smoothing



Time Distortion Anonymization for the Publication of Mobility Data with High Utility. V. Primault, et. al, Proc. IEEE TrustCom'15.

Future Directions: Path confusion



More Details

http://liris.cnrs.fr/privamov

- **Time Distortion Anonymization for the Publication of Mobility Data with High Utility**. V. Primault, S. Ben Mokhtar, C. Lauradoux, L. Brunie. In the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom'15). 2015.
- **Privacy-preserving Publication of Mobility Data with High Utility**. V. Primault, S. Ben Mokhtar & L. Brunie (2015). In the 35th International Conference on Distributed Computed Systems (short)(IEEE ICDCS'15). 2015.
- **Differentially Private Location Privacy in Practice**. V. Primault, S. Ben Mokhtar, C. Lauradoux, L. Brunie. In Mobile Security Technologies Workshop, co-located with 35th IEEE Security and Privacy Symposium. 2014.

Questions?