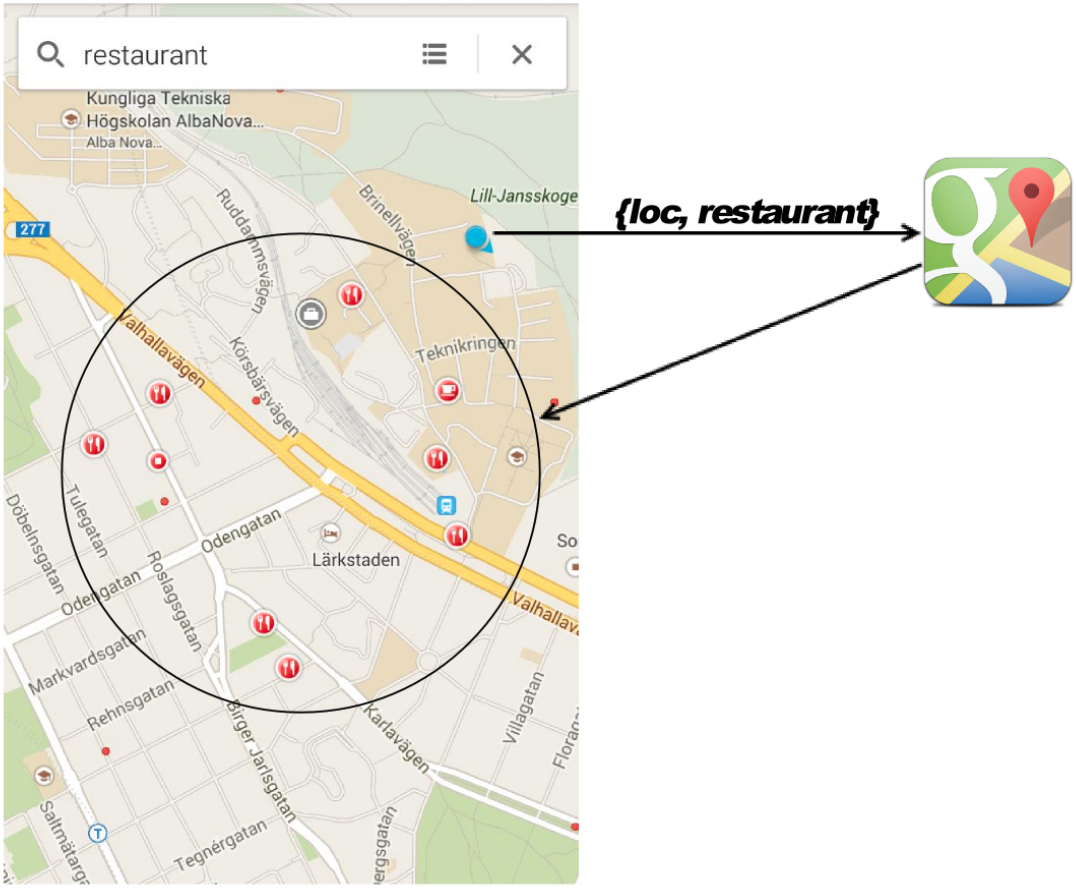
# Resilient Collaborative Privacy for Location-Based Services

Hongyu Jin and Panos Papadimitratos

Networked Systems Security Group
KTH Royal Institute of Technology
Stockholm, Sweden
www.ee.kth.se/nss

NordSec
October 20, 2015

# Background

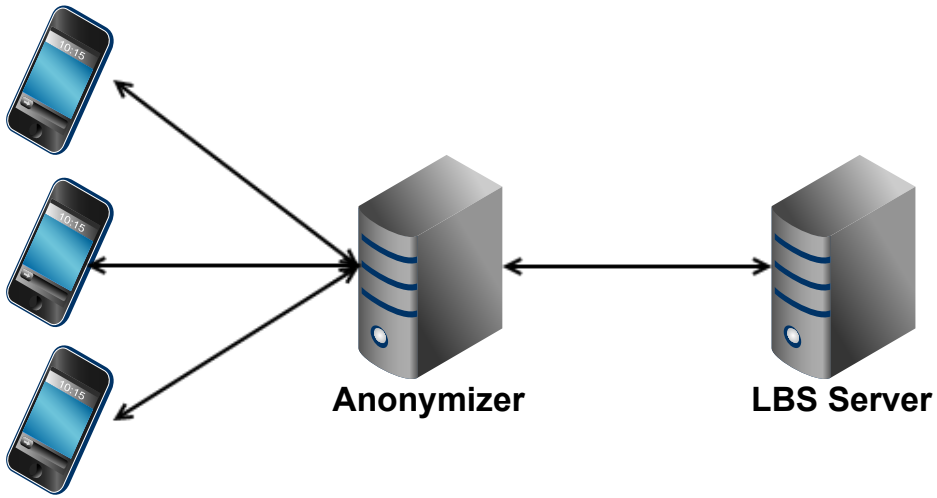



- **Privacy issue** - Expose users (and their queries) to honest-but-curious Location-based Service (LBS) servers

# What can go wrong?

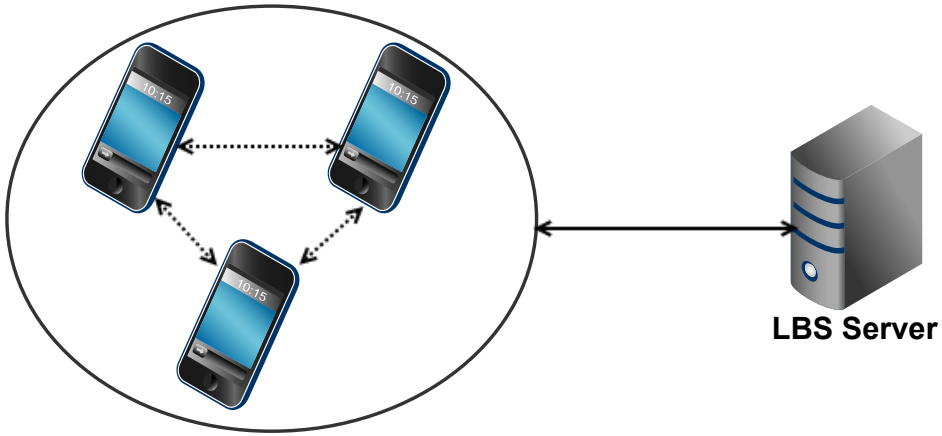
- Location information used to reconstruct user trajectories
- Profile users' activities and infer their interests
- Push advertisements to users

# Centralized Privacy Protection Scheme




- Scheme
  - All the queries are sent to the anonymizer
  - Apply privacy-enhancing technologies on the anonymizer
- Advantages
  - Effective
  - Transparent to client
- Problem
  - Why couldn't an anonymizer also breach the user privacy the same way?

# Decentralized Scheme

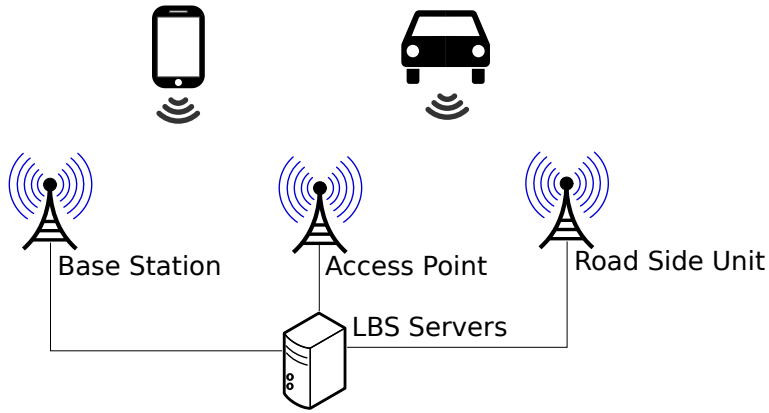



- Objectives
  - Rely on neighbors/peers
  - Contact the LBS server directly, but with protected (anonymized) information
- Example (MobiCrowd [Sho+14])
  - Cache signed results from LBS server
  - Query neighbors first, and query LBS server if no result from neighbors
- Challenge
  - Expose users to faulty or misbehaving nodes

# Security and Privacy Requirements

- Authentication and Integrity
- Non-repudiation and Accountability
- Anonymity/Pseudonymity and Unlinkability
- Confidentiality (optioanlly) - might be required for subscriber-based LBSs

# System Model

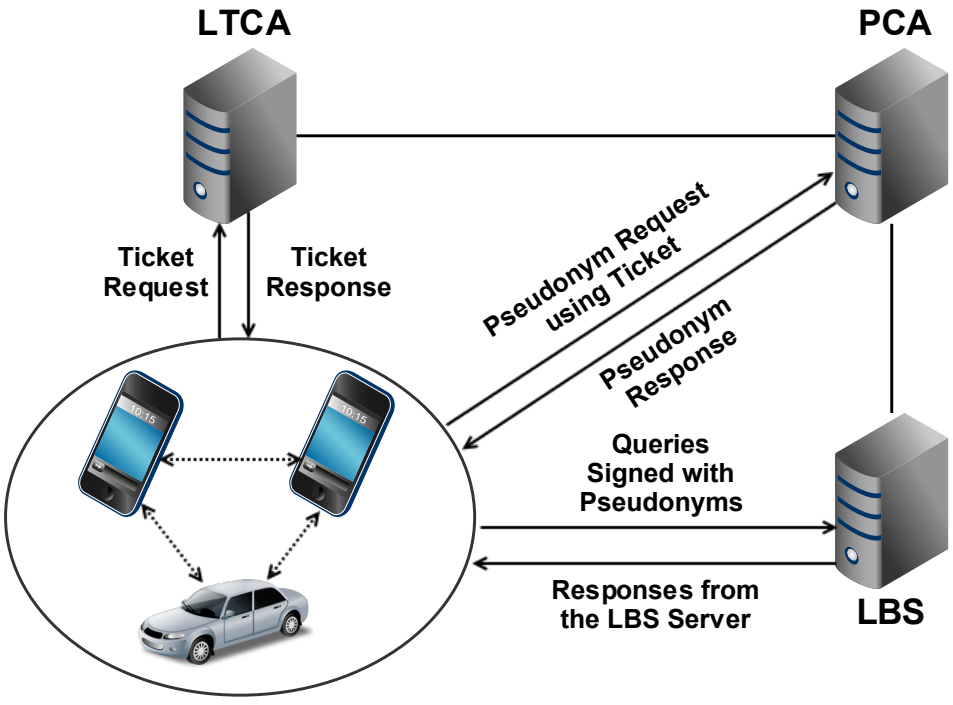



- Nodes (smartphones or On-board Units) are interested in POI information
- Nodes request POI information from LBS servers through the Internet
- Nodes are able to exchange information in an wireless ad-hoc network

**Adversary:**

- LBS servers are honest-but-curious
- Any trusted-third-party introduced could also be honest-but-curious, including the ones we introduce in our scheme
- Nodes can be honest-but-curious
- Nodes can be malicious: deviate from the collaborative protocol functionalities and policies

# Our Scheme




- Client registration with a Long-Term Certification Authority (LTCA)
- Ticket and pseudonym acquisition from LTCA and Pseudonymous Certification Authority (PCA) [Kho+14]
- Leverage information sharing in wireless ad-hoc network
- Pseudonymous authentication for queries and responses
- Pseudonym resolution in case of misbehavior (conditional anonymity)

# Optimizations for Query Processing

- Certificate omission [CaI+11]
  - Omit attaching pseudonyms to reduce communication overhead
- Cache responses to popular queries
  - Such information is likely to become useful later, thus avoid duplicated work
- Set a threshold, $N$, for the number of responses needed
  - Overhear open transmissions and respond in case less than $N$ response are overheard
  - Send an ACK when enough responses are received

# Security and Privacy Analysis

- **Authentication, Integrity, and Confidentiality**
  - Pseudonymous authentication
  - Session key negotiation
- **Non-repudiation and Accountability**
  - Pseudonym resolution
- **Unlinkability**
  - Messages only linkable over pseudonym lifetime, $\tau$

# Security and Privacy Analysis (cont'd)

- **Node Authentication and Exposure to the LBS Server**
  - Pseudonymous authentication
  - Reduced exposure to the LBS server due to collaboration
- **Non-verifiable Responses**
  - Redundant ($N$) responses can help for cross-checking
- **Thwarting Clogging Attacks**
  - Limit the usage of pseudonym
  - Prevent Sybil attack from the infrastructure (PKI) [Kho+14]

# Security and Privacy Analysis (cont'd)

- **Exposure to the Security Infrastructure and Collusion with the LBS**
  - A single LTCA or PCA cannot trace a user's actions [Kho+14]
  - LTCA + LBS: no extra information
  - PCA + LBS: link the batch of pseudonyms obtained from one pseudonym request and the messages authenticated with them
  - Only the collusion of the LBS server, the LTCA and the PCA would expose users

# Performance Evaluation

- **Specifications**
  - Sony Xperia Ultra Z with Quad-core 2.2 GHz Krait 400 CPU
  - Bouncy Castle library for crypto operations (only one available in Android for ECDSA)

**Processing delay of cryptographic operations**

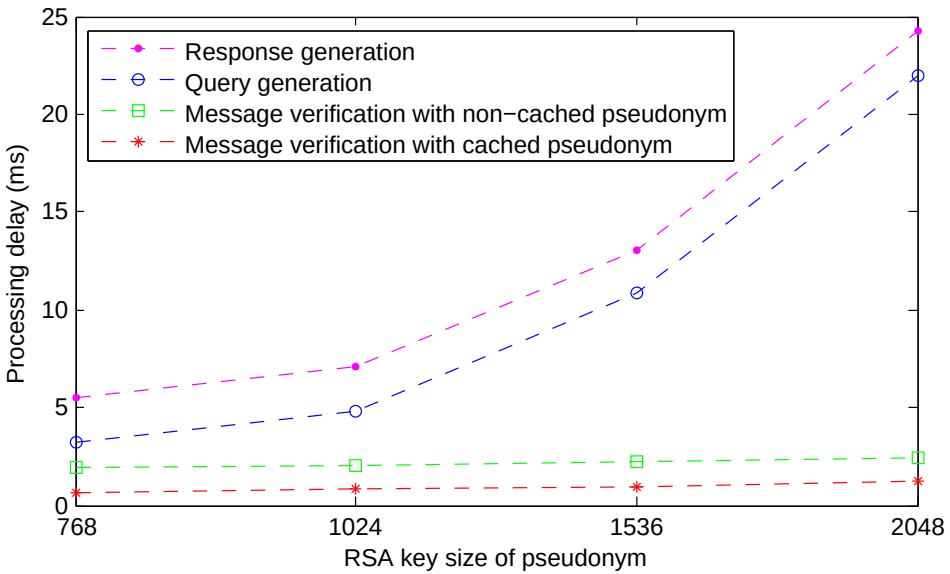
| **Key Type** | **Security Level** (bits) | **Generation** (ms) | **Sign** (ms) | **Verify** (ms) | **Signature Size** (bytes) |
|---|---|---|---|---|---|
| RSA-1024 | 80 | 400.86 | 4.63 | 0.78 | 128 |
| RSA-2048 | 112 | 2104.59 | 21.18 | 1.21 | 256 |
| ECDSA-192 | 96 | 214.65 | 210.01 | 286.44 | 56 |
| ECDSA-224 | 112 | 251.66 | 251.91 | 345.95 | 63 |

- **Key choice - RSA-1024**
  - 80-bit security level
  - Unoptimized ECDSA crypto operations in the library
  - Longer pseudonym lifetime due to lower message rate, implies less key generation

# Performance Evaluation (cont'd)

**Processing overhead for different operations**

| Operation | Processing Overhead |
|---|---|
| **Message verification with cached pseudonym** | Message Verification |
| **Message verification with non-cached pseudonym** | Pseudonym Verification, Message Verification |
| **Query generation** | Message Signing |
| **Response generation** | Database Query, Message Signing |




**Processing delay of different operations, assuming RSA-2048 certificate of the PCA**

- 3000 mobile phone users per $km^2$ in Barcelona [Lou+14]
- Around 100 neighbors assuming Wi-Fi radio range of 100 $m$
- 1.7 $queries/sec$ received assuming 1 $query/min$ per user

# Conclusions

- Decentralized secure and privacy protection scheme for LBSs
- Leverage information sharing in P2P systems
- High resiliency to different attacks and high practicality for deployment
- Can be extended in terms of proposed optimizations

# References


R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J.-P. Hubaux. "Hiding in the Mobile Crowd: Location Privacy through Collaboration". In: *IEEE TDSC* (2014).

G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy. "On the performance of secure vehicular communication systems". In: *IEEE TDSC* (2011).

M. Khodaei, H. Jin, and P. Papadimitratos. "Towards deploying a scalable & robust vehicular identity and credential management infrastructure". In: *IEEE VNC*. Paderborn, Germany, Dec. 2014.

T. Louail, M. Lenormand, O. G. Cantu Ros, M. Picornell, R. Herranz, E. Frias-Martinez, J. J. Ramasco, and M. Barthelemy. "From mobile phone data to the spatial structure of cities". In: *Scientific Reports* (June 2014).