KTH Electrical Engineering

Secure and Privacy-enhancing Location-based Services

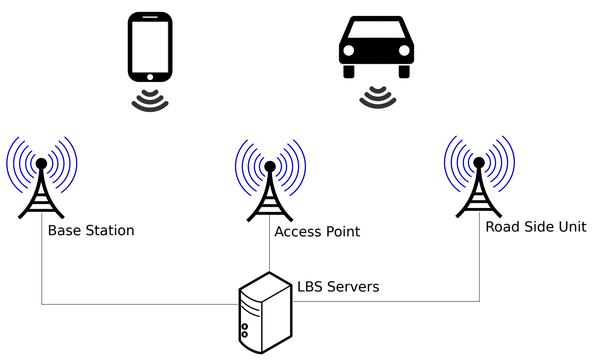
Hongyu Jin, Mohammad Khodaei and Panos Papadimitratos

Networked Systems Security Group
Royal Institute of Technology, Stockholm, Sweden

Abstract

Location-based Services (LBSs) provide convenient features offering valuable services to users. However, the information disclosed through each request harms user privacy. We are concerned with *honest-but-curious* LBS servers which could, by collecting requests, track users and infer additional sensitive user data. This is the motivation of *MobiCrowd*, a *decentralized* location privacy protection scheme for LBSs: users hide themselves from the LBS server, while still getting useful information from their peers. However, such an open data sharing system needs to be secured: users should be prevented from manipulating the shared data. We address exactly this problem, by proposing security enhancements for *MobiCrowd* while preserving privacy.

System Model



- User participation through mobile devices or On-board Units (OBUs) in vehicles
- Communication with LBS servers through different types of network connections
- Peer-to-peer communication over an ad-hoc network

Problem Statement

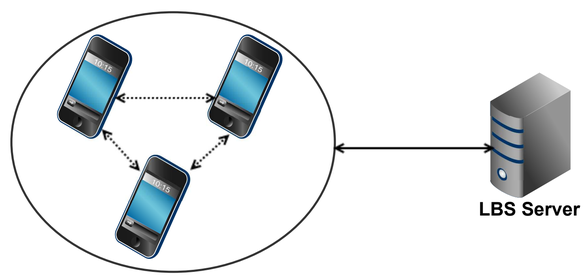
- Assumptions:
  - LBS servers are *honest-but-curious*; they follow the protocols, but they may harm user privacy by profiling or de-anonymizing them.
  - Introduction of a Trusted Third Party (TTP) for query anonymization merely transfers the problem from the LBS server to the TTP.
- Objectives:
  - Disclose as little information as possible to the LBS server.
  - Ensure users obtain useful responses to their queries.

Requirements

- Communication Integrity, Authentication and Confidentiality
- Access Control and Authorization
- Anonymity and Unlinkability
- Non-repudiation and Accountability
- Availability and Scalability

MobiCrowd [1, 2]

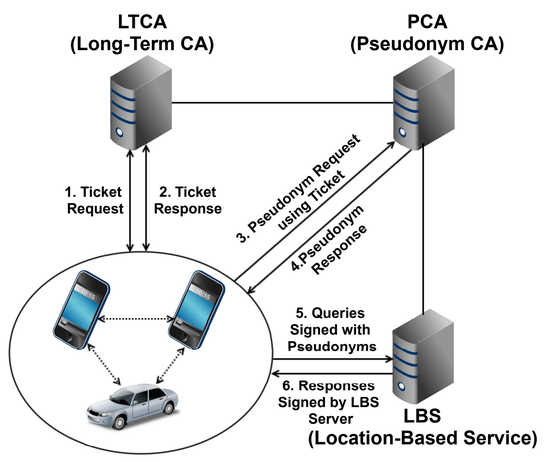
- Basic ideas
  - No need for an anonymization TTP
  - Reliance on peers
  - Contact the LBS server only when absolutely necessary
  - Easy & Simple to implement
- Scheme on the client side
  - Cache signed responses received from the LBS server
  - Query neighbors (peers) first; query the LBS server if the responses from the neighbors do not meet the client requirements/needs



How to Strengthen MobiCrowd?

- Pseudonymous authentication instead of authentication with long-term credentials in order to hide the client identity from the LBS server
- Client-to-client authentication to prevent abuse from peers
- Accountability for peers to protect the system from misbehaving clients

Proposed Scheme



- Client registration with a Long-term Certification Authority (LTCA)
- Ticket and pseudonym acquisition through steps 1-4 [3, 4]
- Pseudonymous authentication for queries
- Pseudonym resolution in case of misbehavior (conditional anonymity)

Our Improved Solution

- Client-to-LBS/client-to-client authentication in a privacy-preserving manner
- Low complexity implemantation; applicable to resource-constrained devices
- Transparency for LBS servers
- Benefit: Increased user/client protection; thus, higher motivation for user participation

Next Steps

- Security & Privacy analysis
- Performance evaluation
- Integration with incentive schemes

References

[1] R. Shokri, P. Papadimitratos, G. Theodorakopoulos, and J.-P. Hubaux. Collaborative location privacy. In *IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)*, Valencia, Spain, October 2011.

[2] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J.-P. Hubaux. Hiding in the mobile crowd: Location privacy through collaboration. *IEEE Transactions on Dependable and Secure Computing*, 11(3):266–279, May 2014.

[3] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos. Vespa: Vehicular security and privacy-preserving architecture. In *Proceedings of the ACM workshop on Hot topics on wireless network security and privacy (HotWiSec)*, Budapest, Hungary, April 2013.

[4] N. Alexiou, S. Gisdakis, M. Laganà, and P. Papadimitratos. Towards a secure and privacy-preserving multi-service vehicular architecture. In *IEEE International Symposium and Workshops on World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Madrid, Spain, June 2013.