

POIsafe: a Privacy-Conscious System for Retrieval of Points of Interest

Daniele Riboni, Linda Pareschi, Claudio Bettini

Università degli Studi di Milano

EveryWare Lab

<http://everywarelab.dico.unimi.it>





Privacy for context-aware services

- Authenticated access:
 - Service requests may contain sensitive information
 - Obfuscation-based techniques, e.g.:
 - R. Wishart et Al., “Context Privacy and Obfuscation Supported by Dynamic Context Source Discovery and Processing in a Context Management System”, UIC, 2007
- Anonymous access:
 - Data in requests may be used to re-identify the issuer
 - Anonymity-based techniques, e.g.:
 - P. Kalnis et Al., “Preventing location-based identity inference in anonymous spatial queries., TKDE 19(12), 2007
- Anonymity and obfuscation can be combined, and coupled with access control, e.g.:
 - L. Pareschi et al., “Composition and Generalization of Context Data for Privacy Preservation”, CoMoRea, 2008

Privacy in a system for POIs

- Objective: to protect against different adversary models
 - The adversary knows the defense method and parameters
 - The adversary may know the identity of request issuers
 - The adversary may know the context of (some) users
 - ...
- Method: enforcing both anonymity and obfuscation at the client-side
 - The exact user's location L is perturbed; the adversary may only derive that L belongs to an area A
 - Obfuscation: A is greater than a given threshold
 - Anonymity: A contains at least N potential issuers

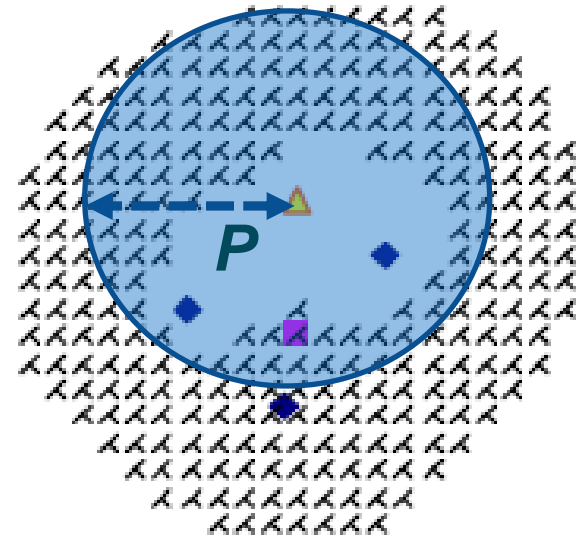
Techniques for privacy in LBS

- SpaceTwist (ICDE'08):
 - Obfuscation-based technique providing exact answer to k NN LBS queries
 - LBS requests are incrementally sent to the server
 - The adversary derives an area from which requests may have been sent (the *twisted space*)
- AnonTwist (MobiUS'09):
 - A modification of SpaceTwist to enforce anonymity
 - Given a (probabilistic) density map, the twisted space contains at least N potential issuers



Shortcoming of existing techniques

- Both SpaceTwist and AnonTwist assume that the function for location obfuscation is unknown
- Without this assumption, the adversary may be able to restrict the area containing the user's location
- Example:
 - The location perturbation is at most P
 - The possible area is the intersection between the blue circle and the twisted space



The *POIsafe* technique

- The perturbation radius and anonymity level (number N of users) are chosen according to users' preferences
- The client incrementally asks for POIs until:
 - The exact k NN set is retrieved
 - The intersection area I is greater than the desired threshold
 - I contains at least N users according to the density map
- If the above conditions cannot be met after a predefined TTL, the client stops sending requests

Future work

- Thoroughly studying the formal properties of POIsafe
- Extending privacy protection to other context data
- Considering other adversary models
 - The adversary has prior knowledge about the association among users and specific values of service parameters
 - The adversary may observe requests issued by multiple users in different time granules