N location diversity +k anonymities: a stronger privacy protection for Users of Location Based Service

Juncheng Pan

project Background

In Location Based Service (LBS) scenario, the location information of user is indispensable input for the service. However the exact location information can exposes user's location related privacy. Most traditional methods is based on spatial k-anonymity cloaking aiming to protect user's query privacy. However, all of the existing work fails to take the privacy of location attributes of users into account.

project Goal

1. Protect user's Location Attributes privacy while guarantee the user's traditional location related privacy.
2. Guarantee the LBS service to be usable and have a well performance.

My contributions to the project

1) We **discovered a new type of privacy attack against user's privacy**, termed user's *location attribute leakage*, on which traditional privacy preserving measures, such as k-anonymity, fail to give an effective protection.

2) After that, we **proposed a novel privacy property**, *N location diversity & K-anonymity*, which offers an effective guide for devising a privacy protection scheme for users.

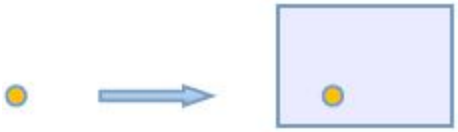
3) We **proposed a novel metric to evaluate and quantify user's privacy level** in terms of the new privacy property based on Voronoi diagrams**.**

4) We **developed some novel algorithms to guarantee the new privacy property** for user based on quad tree, R-tree and Voronoi diagrams.

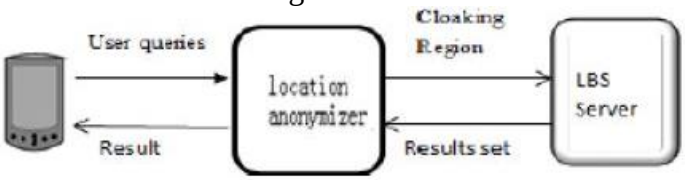
5) We **find and prove some interesting rules about voronoi diagram** which can be used to efficiently compute user's location data's privacy level based on quantified index in my work

The workflow and Technique

1) Choosing a general method to the problem:
Spatial cloaking method: Enlarge the user's exact location to a generalized region.



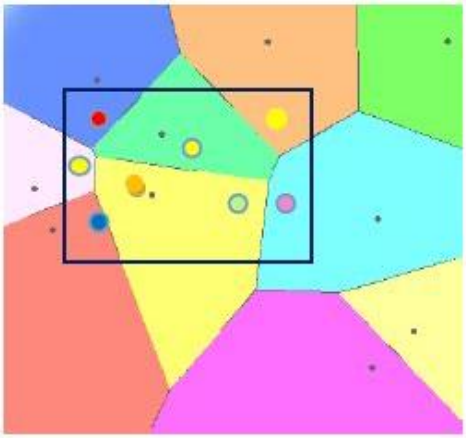
exact location generalized location



We introduce the middle ware (location anonymizer) architecture to in charge of the spatial

2) Quantify the user's privacy level in terms of the new privacy.

N Location diversity and K-anonymity (NLDK): If the generalized location (cloaking region) contains K others users and intersect with N Voronoi Cells of Voronoi diagram of given Public sites, then we say the cloaking region satisfy NLDK property.



example of *7 location diversity and 8 anonymity*

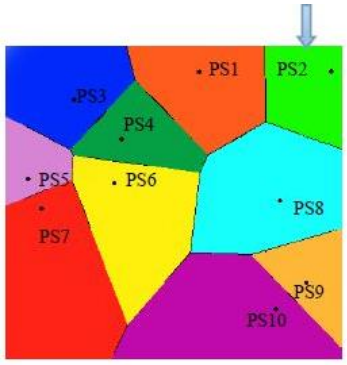
3) Forming a secure NLDK cloaking region for user.

(1). Protecting query privacy: Attacker can't tell specific user who issue LBS service query from k or more potential users above probability of 1/k. (2). Protecting location attribute privacy: Attacker can't tell the specific Location Attribute (LA: The seed of the voronoi Cell in which the user is located) above probability of 1/N.

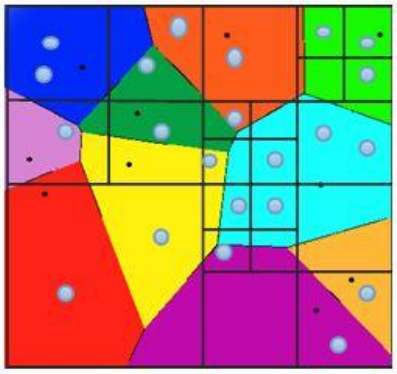
There are three steps to forming NLDK cloaking region for users:

a) **Partition the space**

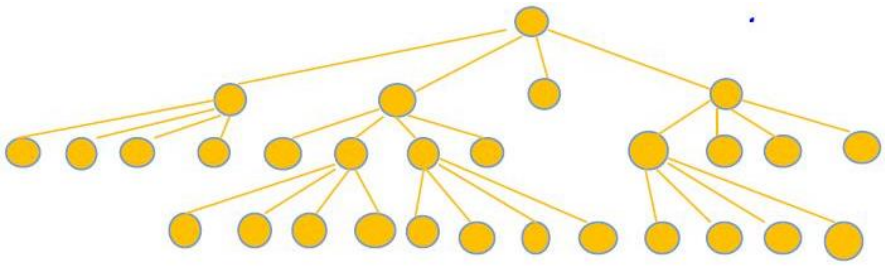
a,1) *patition the space using voronoi diagram using Public sites(PS) as seeds*



a.2) *partition the space using quadtree according to the user distribution in the region*



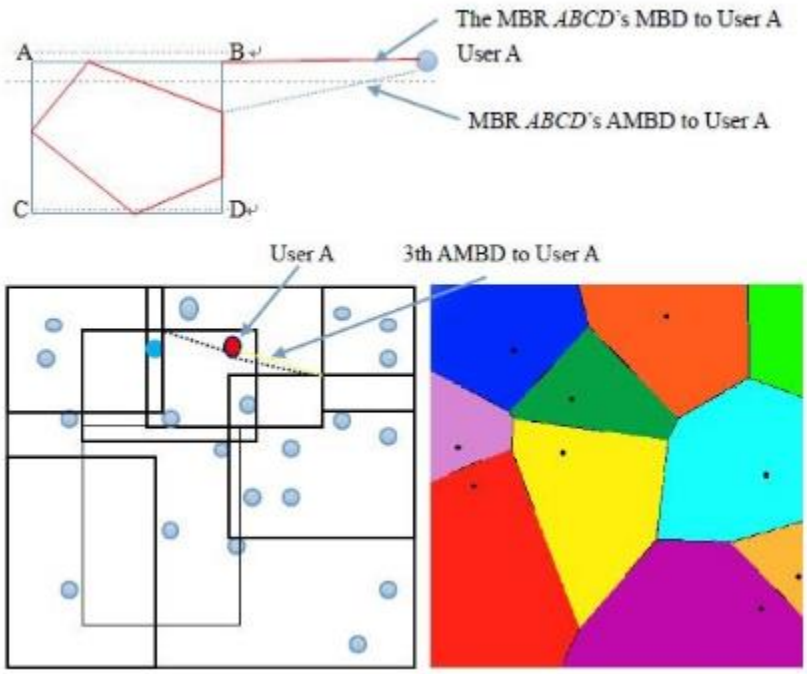
(small blue circles represents the users' distribution)



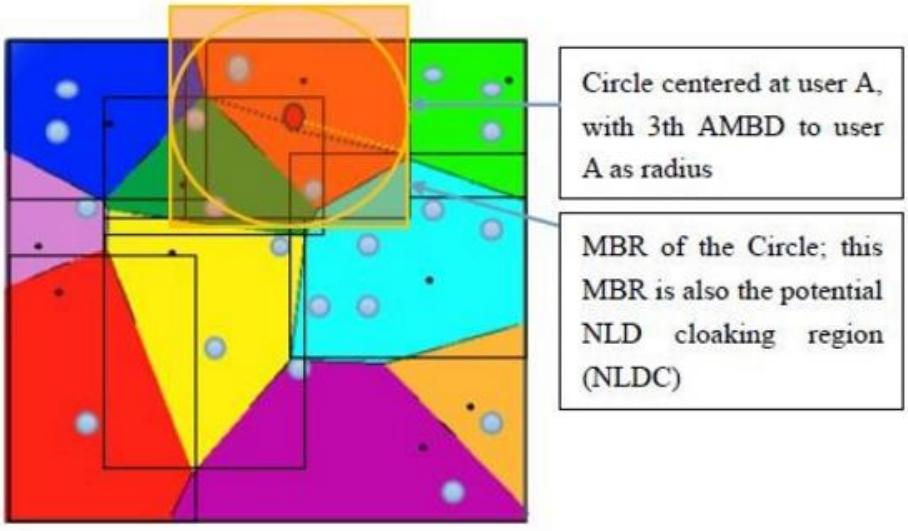
(The yellow nodes represents the quadrand nodes)

b) **Forming a NLD (N location diversity) cloaking region for user.**

b.1)*Bounding every Voronoi cell, and sorting them according to MBD to the User A*

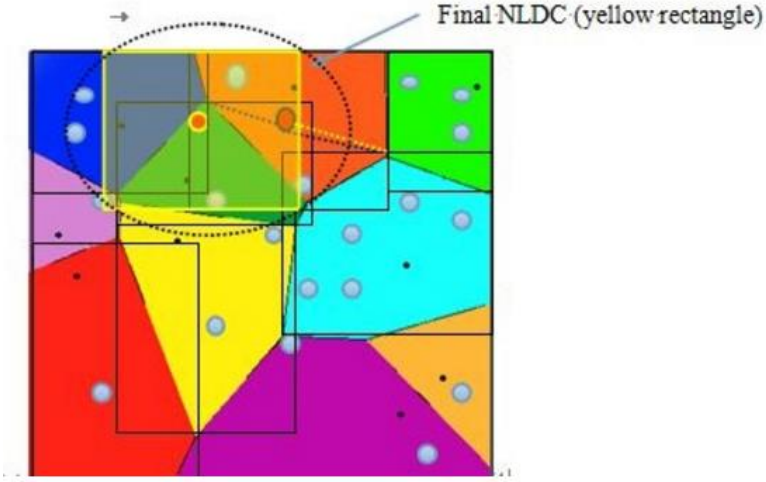


b.2) *Form NLD cloaking region*



The NLDC region formed above is vulnerable to Central PS attack

b.3) *The final NLDC generated by our Secure NLDC*:



C) Render the NLD cloaking region to satisfy k-anonymity