Secure Proximity Queries in Mobile Geo-Social Services

LI Hong Ping

A thesis submitted in partial fulfillment of the requirements for the degree of
Master of Philosophy

Principal Supervisor: Dr. Jianliang XU
Hong Kong Baptist University
August 2012
Abstract

Mobile geo-social networking services are believed to be the killer application for the next-generation mobile computing. A basic service in mobile geo-social networks is the proximity service, which alerts a mobile user when any of his/her friends is in the geographical vicinity, so as to enrich social activities such as collaborative working and information sharing. To realize such services, existing systems collect location information from mobile users for proximity computation. However, the disclosure of private location information to the service provider raises severe privacy concerns. In this thesis, we propose and develop two novel privacy-preserving solutions for mobile proximity query and monitoring services. More specifically, we propose a dynamic-grid-overlay solution for distance-based proximity services and a secure-line-computation solution for vicinity-region-based proximity services. Efficient location update and query reevaluation algorithms for monitoring proximity services are also developed for both solutions. Simulation results demonstrate that our proposed solutions are effective and scalable under various system settings and user moving speeds.
# Table of Contents

Decloration i  
Abstract ii  
Acknowledgements iii  
Table of Contents iv  
List of Tables vi  
List of Figures vii  

1 Introduction  
   1.1 Mobile Geo-Social Networks and Privacy Concerns 1  
   1.2 Proximity Services in Mobile Geo-Social Networks 3  
   1.3 Thesis Organization 6  

2 Related Work  
   2.1 Location Privacy Protection for Query Issuers 7  
   2.2 Location Privacy Protection for both Query Issuers and Queried Objects 9  

3 Privacy-Preserving Distance-based Proximity Services 12
# 3.1 Static Proximity Detection with Location Anonymity

## 3.1.1 Grid Overlay

# 3.2 Dynamic Proximity Monitoring with Location Anonymity

## 3.2.1 Signature Update

## 3.2.2 Query Reevaluation

# 3.3 Performance Evaluation

## 3.3.1 Evaluation Results

# 4 Privacy-Preserving Vicinity-Region-based Proximity Services

## 4.1 Problem Definition and Assumption

## 4.2 Static Proximity Detection with Location Privacy Protection

### 4.2.1 Shift-and-Compare Protocol

### 4.2.2 Analysis of the Shift-and-Compare Protocol

## 4.3 Monitoring of Continuous Proximity Queries

## 4.4 Performance Evaluation

### 4.4.1 Results for Static Proximity Queries

### 4.4.2 Results for Continuous Proximity Monitoring

# 5 Conclusions and Future Work

# Curriculum Vitae