

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

LÊ HOÀNG LONG

MỘT SỐ THUẬT TOÁN ĐẢM BẢO TÍNH RIÊNG TƯ  
TRONG HỆ THỐNG LBS

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Thái Nguyên - 2014

## MỤC LỤC

MỤC LỤC.....	1
DANH MỤC CÁC TỪ VIẾT TẮT .....	5
DANH MỤC HÌNH ẢNH .....	7
PHẦN MỞ ĐẦU.....	10
CHƯƠNG I: TỔNG QUAN VỀ LOCATION BASED SERVICES .....	13
1.1 Định nghĩa Location Based Services .....	13
1.2 Thành phần trong LBS .....	14
1.3 Ứng dụng của LBS.....	15
1.4 Hệ tọa độ địa lý .....	16
1.5 Tính khoảng cách giữa các tọa độ địa lý.....	18
1.6 Tổng quan về tính riêng tư trong LBS .....	19
1.6.1 Tính riêng tư.....	19
1.6.2 Ngữ cảnh – Tính riêng tư trong môi trường ngữ cảnh động .....	20
1.7 Nguy cơ bảo mật tính riêng tư trong LBS .....	21
CHƯƠNG II: MỘT SỐ THUẬT TOÁN VÀ KỸ THUẬT BẢO VỆ TÍNH RIÊNG TƯ CHO LBS .....	23
2.1 Tổng quan về kiến trúc hệ thống bảo vệ tính riêng tư .....	23
2.2 Các nhóm kỹ thuật bảo vệ tính riêng tư.....	25
2.3 Thuật toán và kỹ thuật bảo vệ tính riêng tư .....	27
2.3.1 Kỹ thuật mở rộng câu truy vấn .....	27
2.3.1.1 Mở rộng vị trí tọa độ thành vị trí vùng.....	27
2.3.1.2 Mở rộng vị trí vùng thành vị trí vùng khác .....	28
2.3.1.3 Các dịch vụ về vị trí gần nhau .....	29
2.3.2 Kỹ thuật che giấu không gian .....	31
2.3.2.1 Nhóm giải pháp k-anonymity .....	31
2.3.2.2 Thuật toán Grid.....	33

2.3.2.3 Thuật toán Interval Cloaking .....	35
2.3.2.4 Thuật toán nearest neighbor ASR (nnASR) .....	38
2.3.3 Kỹ thuật làm rối thông tin ( <i>obfuscation technique</i> ).....	39
2.3.3.1 Sinh vật giả .....	42
2.3.3.2 Thuật toán di chuyển trong một vùng lân cận .....	42
2.3.3.3 Thuật toán di chuyển trong một vùng giới hạn lân cận .....	43
2.4 Một số mô hình tấn công tính riêng tư và phương pháp chống .....	45
2.4.1 Mô hình tấn công dựa vào sự phân bố của của các user.....	46
2.4.1.1 Location distribution attack .....	46
2.4.1.2 Phương pháp chống tấn công.....	47
2.4.1.3 Thuật toán CliqueCloak .....	48
2.4.2 Mô hình tấn công dựa vào khả năng di chuyển của user.....	52
2.4.2.1 Maximum movement boundary.....	52
2.4.2.2 Kỹ thuật Patching .....	53
2.4.2.3 Kỹ thuật Delaying.....	53
2.4.2.4 So sánh độ hiệu quả giữa patching và delaying .....	54
2.4.2.5 Thuật toán IcliqueCloak .....	56
2.4.3 Mô hình tấn công dựa vào lịch sử các truy vấn.....	58
2.4.3.1 Query Tracking Attack.....	58
2.4.3.2 Giải pháp để ngăn chặn sự tấn công .....	60
2.4.3.3 Thuật toán m-InvariantCloak.....	61
CHƯƠNG III: CHƯƠNG TRÌNH MÔ PHÒNG .....	65
3.1 Các công nghệ đã sử dụng .....	65
3.1.1 Lập trình web .....	65
3.1.1.1 Sơ lược về .Net Framework.....	65
3.1.1.2 Giới thiệu về ASP.Net .....	66
3.1.1.3 SQL và hệ quản trị cơ sở dữ liệu SQL Server .....	67
3.1.2 Google Maps API .....	67

3.1.2.1 Google Maps Javascript API v3 .....	68
3.1.2.2 Google Maps API Web Services .....	68
3.1.2.3 Google Maps Android API v2.....	69
3.1.3 Xây dựng ứng dụng trên di động .....	69
3.1.3.1 Ngôn ngữ lập trình Java.....	69
3.1.3.2 Hệ điều hành Android.....	70
3.2 Xây dựng mô hình thử nghiệm .....	71
3.2.1 Phân tích lựa chọn mô hình .....	71
3.2.2 Thiết kế hệ thống .....	72
3.2.2.1 Mô hình hệ thống.....	72
3.2.2.2 Biểu đồ Ca sử dụng (Use case) của hệ thống .....	75
3.2.2.3 Biểu đồ triển khai hệ thống.....	77
3.2.3 Xây dựng hệ thống.....	78
3.2.3.1 Ứng dụng cho người dùng cuối .....	78
3.2.3.2 Ứng dụng quản trị hệ thống.....	80
KẾT LUẬN .....	83
TÀI LIỆU THAM KHẢO.....	85

**DANH MỤC CÁC TỪ VIẾT TẮT**

<b>STT</b>	<b>Từ viết tắt</b>	<b>Tiếng Anh</b>	<b>Tiếng Việt</b>
1	3G	Third-generation technology	Công nghệ truyền thông không dây thế hệ thứ ba
2	4G	Fourth-generation technology	Công nghệ truyền thông không dây thế hệ thứ tư
3	ADO.Net	ActiveX Data Objects. Net	Tập hợp hướng đối tượng các thư viện cho phép tương tác với nguồn dữ liệu
4	API	Application Program Interface	Giao diện lập trình ứng dụng
5	ASP	Active Server Pages	
6	CSDL		Cơ sở dữ liệu
7	GIS	Geographic Information System	Hệ thống thông tin địa lý
8	GPRS	General Packet Radio Service	Dịch vụ vô tuyến gói tổng hợp
9	GPS	Global Positioning System	Hệ thống định vị toàn cầu
10	HTML	HyperText Markup Language	Ngôn ngữ đánh dấu siêu văn bản
11	J2EE	Java Enterprise Edition	Nền tảng lập trình dành cho việc phát triển ứng dụng
12	JSON	JavaScript Object Notation	Một kiểu dữ liệu trong JavaScript

13	LBA	Location-based Application	Ứng dụng có sử dụng thông tin vị trí
14	LBS	Location-based Services	Dịch vụ dựa trên vị trí địa lý
15	MBR	Minimum Boundary Rectangle	Hình chữ nhật bao nhỏ nhất
16	MMB	Maximum Movement Boundary	Vùng bao vị trí chính xác của người dùng
17	OOP	Object-oriented programming	Lập trình hướng đối tượng
18	PDA	Personal Digital Assistant	Thiết bị kỹ thuật số hỗ trợ cá nhân
19	RDBMS	Relational Database Management System	Hệ thống quản trị cơ sở dữ liệu quan hệ
20	SP	Service Provider	Nhà cung cấp dịch vụ
21	SQL	Structured Query Language	Ngôn ngữ truy vấn mang tính cấu trúc
22	TCP/IP	Transmission Control Protocol/Internet protocol suite	Bộ giao thức liên mạng
23	WLAN	Wireless local area network	Mạng cục bộ không dây
24	WORA	“Write once, Run anywhere”	“Viết 1 lần, sử dụng ở bất kỳ đâu”

## DANH MỤC HÌNH ẢNH

Hình 1-1: LBS là sự kết hợp của nhiều công nghệ [4].....	13
Hình 1-2: Các thành phần cơ bản của LBS.....	14
Hình 1-3: Một số phân loại của các ứng dụng LBS [16] .....	16
Hình 1-4: Bản đồ Trái Đất với vĩ tuyến (ngang) và kinh tuyến (dọc) .....	18
Hình 1-5: Các kiểu ngữ cảnh khác nhau theo Nivala(2003).....	20
Hình 2-1: Kiến trúc không hợp tác [12].....	23
Hình 2-2: Kiến trúc tập trung [12] .....	24
Hình 2-3: Kiến trúc ngang hàng [12] .....	25
Hình 2-4: Quy trình hoạt động của hệ thống Cloaking Agent [14] .....	28
Hình 2-5: Vị trí thật và vị trí bị che giấu.....	28
Hình 2-6: Mở rộng vị trí từ vùng sang vùng [5] .....	29
Hình 2-7: Xác định điểm lân cận của A [15] .....	30
Hình 2-8: k-anonymity (k=10).....	32
Hình 2-9: Minh họa giải thuật Grid.....	34
Hình 2-10: Quy trình chọn ra vùng 5-anonymity cho điểm tô đồ .....	36
Hình 2-11: Theo dõi quá trình truy vấn dữ liệu .....	37
Hình 2-12: Minh họa giải thuật nnASR .....	38
Hình 2-13: Quy trình hoạt động của hệ thống sử dụng kỹ thuật Dummy [8].....	39
Hình 2-14: Chống theo dõi quá trình truy vấn dữ liệu [8] .....	40
Hình 2-15: Phát sinh thông điệp giả dựa trên mô hình Circle [9].....	41
Hình 2-16: Phát sinh thông điệp giả dựa trên mô hình Grid [9] .....	41
Hình 2-17: Minh họa 2 giải thuật sinh vật giả .....	42
Hình 2-18: Phân bố user.....	47
Hình 2-19: Vùng giới hạn .....	48
Hình 2-20: Vùng làm mờ .....	48
Hình 2-21: Đồ thị giới hạn .....	49
Hình 2-22: Đồ thị l-clique .....	49

Hình 2-23: Maximum movement boundary.....	52
Hình 2-24: Kỹ thuật Patching .....	53
Hình 2-25: Kỹ thuật Delaying.....	54
Hình 2-26: Đồ thị so sánh chất lượng và tính riêng tư của 3 loại kỹ thuật.....	55
Hình 2-27: Đồ thị so sánh thời gian và vận tốc tối đa của 3 loại kỹ thuật.....	55
Hình 2-28: Thời gian cloaking trung bình .....	57
Hình 2-29: Bảng thông tin cư dân.....	59
Hình 2-30: Bảng thông tin suy đoán .....	59
Hình 2-31: Vùng làm mờ 3-anonymity.....	60
Hình 2-32: Mô hình 3-anonymity, 2-diversity, 2-invariance .....	61
Hình 3-1: Thành phần trong các phiên bản .NET Framework (2005 - 2010) ....	66
Hình 3-2: Mô hình hệ thống mô phỏng.....	74
Hình 3-3: Biểu đồ Ca sử dụng của tác nhân Người dùng .....	75
Hình 3-4: Biểu đồ Ca sử dụng của tác nhân Ứng dụng Client .....	76
Hình 3-5: Biểu đồ Ca sử dụng của tác nhân Quản trị viên .....	76
Hình 3-6: Biểu đồ Ca sử dụng của tác nhân Dịch vụ Server .....	76
Hình 3-7: Biểu đồ triển khai hệ thống.....	77
Hình 3-8: Giao diện khởi động ứng dụng .....	78
Hình 3-9: Danh sách các danh mục trong ứng dụng.....	78
Hình 3-10: Giao diện mẫu tìm kiếm địa điểm .....	78
Hình 3-11: Giao diện hiển thị kết quả tìm kiếm .....	78
Hình 3-12: Giao diện mẫu thiết lập vị trí vật giả .....	79
Hình 3-13: Giao diện mẫu cấu hình ứng dụng.....	79
Hình 3-14: Giao diện thông tin ứng dụng .....	79
Hình 3-15: Giao diện trang đăng nhập quản trị .....	80
Hình 3-16: Giao diện danh sách nhóm địa điểm.....	81
Hình 3-17: Giao diện cập nhật thông tin nhóm địa điểm.....	81
Hình 3-18: Giao diện danh sách địa điểm.....	82



Hình 3-19: Giao diện cập nhật thông tin địa điểm..... 82

## PHẦN MỞ ĐẦU

Sự ra đời của các thế hệ điện thoại, các thiết bị di động thông minh, có khả năng kết nối internet, khai thác các dịch vụ đã làm cho các ứng dụng trên chúng ngày càng trở lên phong phú, đa dạng, đặc biệt là các ứng dụng dịch vụ dựa trên vị trí địa lý (Location-based Services - LBS) như các hệ thống dẫn đường, tìm kiếm địa điểm, trò chơi,... Các dịch vụ này đã mang lại nhiều lợi ích, tiện lợi và làm cải thiện cuộc sống của con người. Việc giao tiếp, trao đổi dữ liệu, giới thiệu ý tưởng, mua bán hàng hóa và dịch vụ giữa con người với con người không còn giới hạn biên giới nữa khi mọi việc đều thực hiện thông qua mạng Internet.

Bên cạnh các lợi ích như vậy, các ứng dụng cũng kèm theo những rủi ro và thách thức mới liên quan đến quyền lợi riêng tư của người sử dụng dịch vụ của các ứng dụng trên. Đặc trưng của loại ứng dụng có sử dụng thông tin vị trí (Location-based Application - LBA) là phải theo vết di chuyển của người sử dụng dịch vụ để từ đó xác định được vị trí tương ứng và cung cấp dịch vụ tốt nhất. Việc các thông tin vị trí của người dùng được trao đổi thường xuyên trên mạng gây mất an toàn thông tin vị trí cá nhân. *Tính riêng tư* được đề cập đến như là việc che giấu thông tin vị trí của đối tượng chuyển động khi trao đổi trên mạng. Tính riêng tư được đánh giá đặc biệt quan trọng trong LBS.

Một vài nghiên cứu trong những năm gần đây đã nêu lên những rủi ro bảo mật và tính riêng tư cho người khai thác dịch vụ trực tuyến (như đánh cắp định danh, suy diễn dựa trên thông tin người dùng, bị giám sát trực tuyến và lừa đảo, ...). Chính vì những lý do trên, Tổ chức Hợp tác và Phát triển kinh tế thế giới - OECD (Organisation for Economic Co-operation and Development) đã cảnh báo về vấn đề bảo vệ tính riêng tư trong các giao dịch trên mạng toàn cầu.

Hệ quả của việc sử dụng đa dạng thông tin ngữ cảnh (vị trí địa lý, thông tin cá nhân, sở thích, tốc độ di chuyển, địa hình, sự phân bố dân cư...) trong ứng