International Journal on Applications in Engineering and Technology
Volume 5 : Issue 2: December 2019, pp 1 – 4 www.aetsjournal.com ISSN (Online) : 2455 - 0523

PRIVACY AND PRESERVING MAP LOCATION USING ANDROID APP

T.MANIVEL , GOWRISHANKAR . R

Abstract— As smartphones are increasingly used to run apps that provide users with location-based services. Accessible solutions to this concern are deficient in terms of practicality, efficiency, and effectiveness. A user expects the app to access his location only when a location-based functionality is required, (e.g., localized-search, place check-in, etc. Most Android apps). It's just part of the deal of using their mobile operating systems with location services enabled.

I.INTRODUCTION

Smartphone is packed with sensors, monitoring where you are in the world, how fast user moving through space. Android phone, open the Settings app then go to Apps & notifications, choose an app, and select Permissions.

II. LITERATURE SURVEY

1) "The loss of location privacy in the cellular age," Communications of ACM

Author: S. B. Wicker

The evolution of location-based services (LBS), culminating in Apple's and Google's use of crowdsourced data to create a system for obtaining location fixes potentially faster and more accurate than the global positioning system (GPS).

2) A classification of location privacy attacks and approaches,Personal and Ubiquitous Computing

Author : M. Wernke, P. Skvortsov, F. Durr, and K. Rothermel

Location-based services have become very popular, mainly driven by the availability of modern mobile devices with integrated position sensors.

3) "A Formal Model of Obfuscation and Negotiation for Location Privacy"

Author: Matt Duckham , 2005

This framework provides a computationally efficient mechanism for balancing an individual's need for high-quality information services against that individual's need for location privacy.

4) "A Peer to Peer Spatial Cloaking Algorithm for Anonymous Location based Services"

Author: Chi Yin Chow, 2006

Two modes of operations are supported within the proposed P2P spatail cloaking algorithm, namely, the on-demand mode and the proactive mode

III.EXISTING SYSTEM

Find existing general-purposed location privacy protection mechanisms (LPPMs) not effective, when applied to map service on smartphones.

Experimental results show that ShiftRoute strikes a good tradeoff between location privacy and service usability.

A. DISADVANTAGES

Smart phones can be addictive and spending too much time on them can make you socially isolated from the real world.Storage can be a problem. Smartphones are small so there isn't space for a huge, built-in hard drive.

Smartphones can be expensive, especially those high-end phones with great specs and features.

IV.PROPOSED SYSTEM

As smartphones are increasingly used to run apps that provide users with location-based services.

Location Privacy Guardian (LP-Guardian), accessible approaches by addressing the tracking,

T.Manivel , Assistant Professor , Department of Information Technology , Muthayammal Engineering College.

R.Gowrishankar , Assistant Professor , Department of Information Technology , Muthayammal Engineering College.

profiling, and identification threats while maintaining app functionality.

A user expects the app to access his location only when a location-based functionality is required, (e.g., localized-search, place check-in, etc. Most Android apps).

A. ADVANTAGES

The Global Positioning System (GPS) provides satellite tracking services that are useful in a wide range of commercial and personal applications.

Smartphones evolved from the earliest communication devices.

Most smartphones now are equipped with Global Positioning System (GPS).

V. ARCHITECTURE DIAGRAM

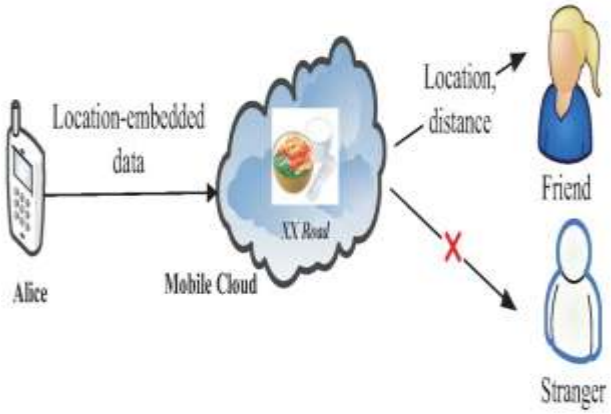


Figure 1:

1) Map Location Monitoring Module

The location monitoring system using identity sensors, the sensor nodes report the exact location information of the monitored persons to the server; thus using identity sensors immediately poses a major privacy breach.

The counting sensors by nature provide aggregate location information, they would also pose privacy breaches.

2) Aggregate locations Module

The design two in-network location anonymization algorithms, namely, resource- and quality-aware algorithms that preserve personal location privacy, while enabling the system to provide location monitoring services.

3) Mapped Location monitoring Module

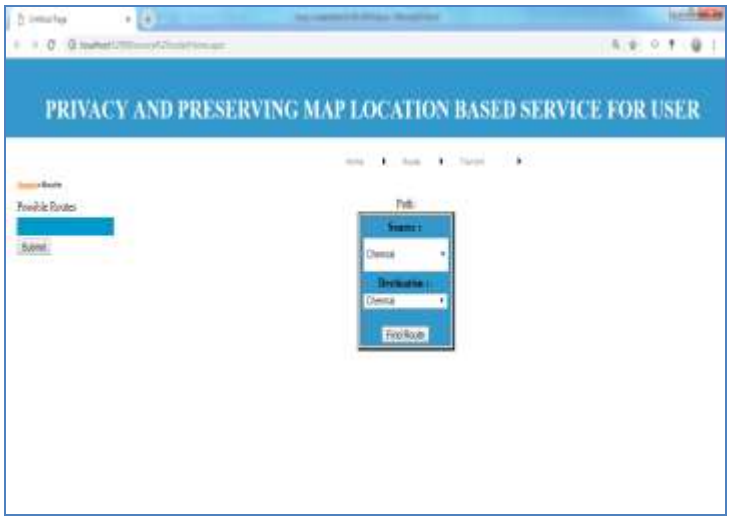
The server is responsible for collecting the aggregate locations reported from the sensor nodes, using a spatial histogram to estimate the distribution of the monitored objects, and answering range queries based on the estimated object distribution. Furthermore, the administrator can change the anonymized level k of the system at anytime by disseminating a message with a new value of k to all the sensor nodes.

4) Minimum bounding rectangle (MBR)

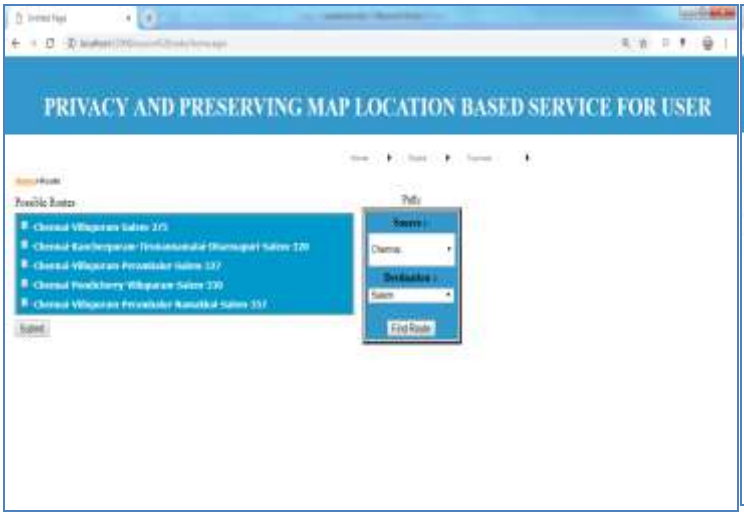
The minimum bounding rectangle (MBR) of the sensing area of A. It is important to note that the sensing area can be in any polygon or irregular shape.

VI. SAMPLE SCREENS

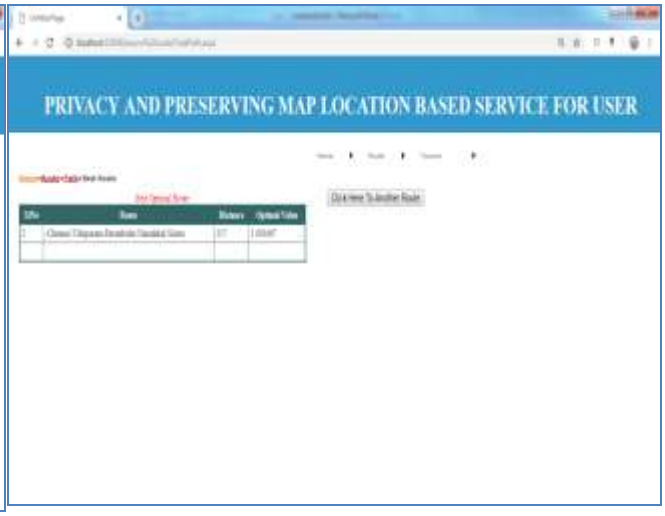
1) HOME PAGE



2) FIND ROUTE

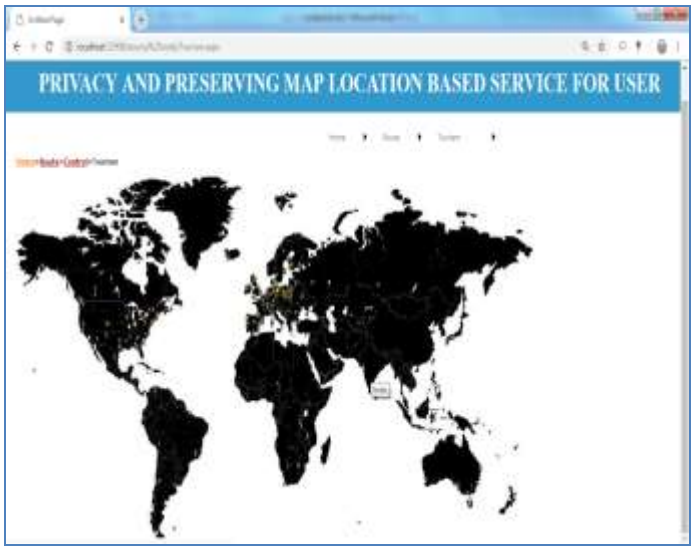


5) BEST ROUTE

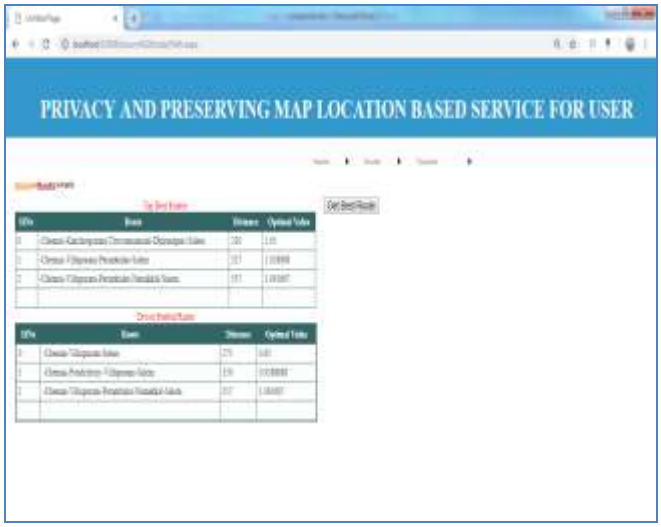


3) POSSIBLE ROUTES

6) LOCATION TOURISM PAGE



4) TOP BEST ROUTES



7) CONTROL CENTER

8) CONTROLLER LOGIN

9) ROUTINGENTRY

VII. CONCLUSION

An improved privacy-preserving framework for location-based services based on double cloaking regions with supplementary information constraints.

Compared to previous work, our method is effective in solving the strong attack with supplementary information, and, comparing to generating random dummy positions, generating fixed ones improves the service quality but reduces the computational overhead for the client..

VIII.FUTURE ENHANCEMENT

The stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods

References

[1] Dr.E.Punarselvam and S.Gopi,"Effective and Efficient Traffic Scrutiny in Sweet Server with Data Privacy", International Journal on Applications in Information and Communication Engineering Volume 5 : Issue 2: November 2019, pp 1 – 5.

[2] Gowrishankar.R , T.Manivel , " Securing wireless devices using location based services", International Journal on Applications in Information and Communication Engineering Volume 5 : Issue 2: December 2019, pp 25 – 32.

[3] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, .The anatomy of a context-aware application,. in Proc. Of MobiCom, 1999.

[4] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, .The cricket location-support system,. in Proc. of MobiCom, 2000.

[5] B. Son, S. Shin, J. Kim, and Y. Her, .Implementation of the realtime people counting system using wireless sensor networks,. IJMUE, vol. 2, no. 2, pp. 63.80, 2007.

[6] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, .Privacy-aware location sensor networks,. in Proc. of HotOS, 2003.

[7] G. Kaupins and R. Minch, .Legal and ethical implications of employee location monitoring,. in Proc. of HICSS, 2005.

[8] Location Privacy Protection Act of 2001, http://www. techlawjournal.com/cong107/privacy/location/s1164is.as..

[9] D. Culler and M. S. Deborah Estrin, .Overview of sensor networks, . IEEE Computer, vol. 37, no. 8, pp. 41.49, 2004.