ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Privacy-Preserving Indoor/Outdoor Localization on Smart Phones

Sudarshan Jagtap, Rahul Kamble, Mahesh Shinde, Sanket Jangale, Prof. Shrinivas D.

Department of Computer Engineering, G.S. Moze College of Engineering, Balewadi, Pune, MH, India

ABSTRACT: Privacy is the most considered factor for the people and is the most important feature the developers to keep in mind while developing the applications. Over the last few decades many research focus on the location privacy but still contradiction and challenges in conquer these risk. The techniques and methodology varied according to the application of location based service. Anonymous location information may be correlated with restricted spaces such as home and office for subject re-identification. This makes it a great challenge to provide location privacy protection for users of location-based services. Location proof of a particular person relies on his/her mobile device position. One of the valuable features of the location proofs tells about accessing the location based services (LBS) by using mobile device. Location privacy is mandatory for every user to keep their location confidential .Every user needs to maintain the privacy level according to their spatial and temporal region. In this paper, we have presented a survey about the various techniques that are well suited to preserve location privacy and location proofs.

KEYWORDS: anonymity, location proof, location privacy, location-based services, localization techniques.

I. INTRODUCTION

Location privacy has been a serious concern for mobile users who use location-based services provided by the third party provider via mobile networks. Mobile Networks are insecure due to its broadcasting nature. A mobile network doesn't have a clear line of protection. So mobile nodes can join the network and leave the network at any time and at any location [1]. The location based services is based on the user location which can be provided by the mobile devices. Loopt and Google latitude are applications used to update the user's current location proof. Location-based services provide information about nearest entities (i.e. Nearby ATM, Restaurants, airports, etc.,) and offer location aware services. Geo-location data is gathered in a number of ways, including built-in Global Positioning System devices, IP address, or Wi-Fi network mapping. Location proof plays a vital role in location sensitive applications. Location sensitive applications such as [3],[10] Location based access control, Location aware routing, etc., are used in location proofs. They are also helpful in providing a history of location proofs and identifying a geographical location of users. Location proof is a piece of data that certifies a receiver to a geographical location [3]. In the location proof updating system, location information can be eavesdropped by adversaries. It may cause vulnerability towards location privacy of the user. Public key Cryptographic operation is used for encryption and decryption of communicating messages and prevents from eavesdropping. The Process of hiding the identity of nodes is an approach to obtain identity privacy; the identity of the node is hidden by using pseudonym.

Literature Survey

Igor Bilogrevic, Murtuza Jadliwala [1] proposed privacy-preserving algorithms for determining an optimal meeting location for a class of users. They perform a thorough privacy valuation by formally computing privacy-loss of the proposed approaches. They deal with the privacy issue in LSBSs by focusing on a explicit problem called Fair RendezVous Point(FRVP) problem. Given a set of user location preferences, this FRVP problem is to find out a location among the proposed ones such that the greatest distance between this location and all other users' locations is minimized. Rinku Dewri and Ramakrishna Thurimella [2] proposed a user-centric location based service architecture where a user can examine the blow of location inaccuracy on the service by deciding the geo coordinates to use in a query. They construct a search application based on user-centric locationbased service architecture where a user can detect the impact of position inaccuracy on the service accuracy. Jing Liu, Zechao Li, Jinhui Tang [3] authors focus on the personalized tag recommendation task and try to recognize user-preferred, geo-locationspecific as well as

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

semantically significant tags for a photo by leveraging rich contexts of the unreservedly existing community-contributed photos. For users and geo-locations, they have different privileged tags assigned to a photo, and recommend a subspace learning method to individually expose the both types of preferences.

Linke Guo, Chi Zhang [4] proposes a privacypreserving revocable content sharing scheme in geosocial networks. Proposed scheme allows mobile users to share their encrypted location-based contents on an untrusted server without revealing genuine location information, and further enables other mobile users who physically check in at the particular location to search and decrypt the content if they have the equivalent attributes. Muhammad Ridhwan Ahmad Fuad and Micheal Drieberg [5] presents the expansion of the remote vehicle tracking system which accommodate the Global System for Mobile Communications (GSM) Modem and Google Map. Wei Xin, Cong Tang, TaoYang [6] uses LocSafe method, a "missed-connections" service is used which grantees based on RFID technology, in order to verify an encounter sharing between users in the past. LocSafe is composed of three parts: RFID Tags, LE Collectors, and social service provider. They use RFID technology to detect encounters, and use attribute-based encryption and broadcast encryption to create conviction and defend users, privacy. We estimate LocSafe by a study of "missedconnections "troubles and study of system implementation. Wei Li, Wei Jiao, Guangye Li [7] LocationBased Service(LBS) combined with mobile devices and internet become more and more trendy, and are widely used in traffic navigation, intelligent logistics and the point of interest query. However, most users worry about their privacy when using the LBS because they should provide their precise location and query content to the undependable server. This paper analyses the query association attack model for the constant query in mobile LBS.

Jianliang Xu, Xueyan Tang [8] identifies and addresses three new issues concerning location cloaking approach. First, study the demonstration of cloaking regions and illustrate that a circular region normally leads to a small result size for region-based queries. Second, extend a mobility-aware location cloaking technique to oppose trace analysis attacks. Two cloaking algorithms, explicitly MaxAccu_Cloak and MinComm_Cloak, are intended based on different performance objectives. Finally, develop an competent polynomial algorithm for evaluating circular-region-based kNN queries Hanunah Othman, Habibah Hashim, Jamalul-lail Ab Manan [9] studies modern schemes deliberate to present location privacy and anonymity to LBS users. The main idea is to decipher current practical problem by proposing a latest framework of LBS Middleware called Trusted Anonymizer (TA) secured by Trusted Computing (TC) technologies. Leone C. Monticone, Richard E. Snow [10] provides an analysis of the case where the MRs operate in or above circular service areas on the surface of a spherical Earth. The analysis provides an accurate and competent way, which is less complex than performing the calculations on the sphere, to compute true minimum distance ratios. The method uses stereographic projection to convert the original minimization problem into a simpler problem of minimizing a ratio of Euclidean distances, which is expressed as a function of a single real variable, over the boundaries of discs (i.e., circles) in the complex plane. V. N. Sahare, Y. Raut, Dr. M.V.Sarode[11] proposed a system which will find out the relative position between several vehicles by using Great Circle Algorithm. The enhancement in VANET connectivity is made by road side unit which will supervise all the vehicle information and detect the failure vehicle and calculate the detail of the vehicles that get affected by the failure vehicle and multicast alert packet to well-known vehicles. This will avoid the broadcasting difficulty**.**

II. PROPOSED WORK

This proposed system will hide the location of users by using stealth geo-synchronization. Great circle algorithm will be use for calculating the distance between multiple geo-locations. Then by using polygon centroid calculation, central point will be determined. This system will provide the central location which will be approximately same for all users by considering user preferences; it will also provide privacy about users location

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

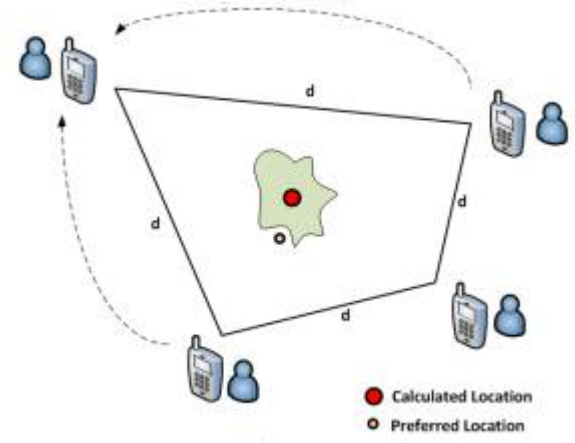

Figure 1: Proposed System Architecture

Above figure shows the overall working process of proposed system. This process includes multiple stages of execution. As per shown consider a condition there are five users in group planning to meet in centrally preferred location then one user from all will become master user and after which all user will share their location with master user and master user will execute the process. After execution system will calculate the central location by calculating the centroid of the polygon created by the user's connection. Once system get the central location it will ask user about his preferred location and after this using Google mapping API system will find out the nearest location selected by the user and once it found system will inform all user about final meeting location and if user wants he can view the travelling path to the location.

III. PROPOSED SOLUTION

From the idea of the proposed system we are clear with two outcomes. These two outcomes are discussed below.
1) Provide central feasible location Central feasible location will be calculated by using great circle algorithm and polygon centroid calculation. Then by using Google map API users location will be track.
2) Provide privacy to all users.
Privacy can be provided by using stealth geo synchronization.

IV. CONCLUSION

In this paper, we proposed a fine-grained Privacy-preserving Location Query Protocol (PLQP), which successfully solves the privacy issues in existing LBS applications and provides various location based queries. The PLQP uses our novel distance computation and comparison protocol to implement semi-functional encryption, which supports multi levelled access control, and used CP-ABE as subsidiary encryption scheme to make access control be more fine-grained. Also, during the whole protocol, unless intended by the location. This system will provide the central location or the location which is nearer to all users by using great circle algorithm and users location will be determined by using Google map API and GSM. Location privacy is the capability to prevent new parties from learning one's present or past location. Generally, Location Based Service (LBS) gives an information service about the physical location of a user. Proposed system will also provide privacy about user's location.

REFERENCES

[1] Igor Bilogrevic, Murtuza Jadliwala, Vishal Joneja," Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices", IEEE Transactions on Information Forensics and Security , Vol. 9, NO. 7,2014. [2] Rinku Dewri and Ramakrishna Thurimella, "Exploiting Service Similarity in Location Based Search Queries, "IEEE Transaction on Parallel and Distributed, February 2014.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

[3] Jing Liu, Zechao Li, Jinhui Tang, "Personalized Geo-Specific Tag Recommendation for Photos on Social Websites", IEEE Transaction on Multimedia, Vol. 16, NO. 3, April 2014.
[4] Linke Guo, Chi Zhang, "Privacy-Preserving Revocable Content Sharing in Geosocial Networks", IEEE Conference on Communication and Network Security,2013.
[5] Muhammad Ridhwan Ahmad Fuad and Micheal Drieberg, "Remote Vehicle Tracking System using GSM Modem and Google Map", IEEE Conference on Sustainable Utilization and Development in Engineering and Technology, 2013 .
[6] Wei Li, Wei Jiao, Guangye Li, "A LOCATION PRIVACY PRESERVING ALGORITHM FOR MOBILE LBS", IEEE CCIS, 2012.
[7] Wei Xin, Cong Tang, Tao Yang,Hui Ping sun, Zhong Chen, "Towards-Privacy Preserving RFID-Based Location Based Services",IEEE International Conference on Fuzzy System and Knowledge Discovery, 2012.
[8] Jianliang Xu, Xueyan Tang, "PrivacyConscious Location-Based Queries in Mobile Environments", IEEE Transactions on Parallel and Distributed Systems , VOL. 21, NO. 3, MARCH 2010
[9] Hanunah Othman, Habibah Hashim, Jamalul-lail Ab Manan, "Privacy Preservation in Location-Based Services (LBS) Through Trusted Computing Technology", IEEE International Conference on Communication, December 2009.
[10] Leone C. Monticone, Richard E. Snow, "Minimizing Great-Circle Distance Ratios of Undesired and Desired Signal Paths on a Spherical Earth", IEEE Transaction on vehicular technology, Vol. 58, NO. 9, November 2009. [11] V. N. Sahare, Y. Raut, Dr. M.V.Sarode, "Early Alert System Using Relative Positioning in Vehicular Ad-hoc Network", International Conference on Magnetics, Machines &