International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue – Active Galaxy
ISSN No: 2456 - 6470 | www.ijtsrd.com | Special Issue Publication

Integrity Assurance with Minimum Location Disclosure on Mobile Devices by Using Pmac

Mr. P. Senthil[1], Mrs. S. DurgaDevi[1], Bhargavi M. B.[2]
[1]Assistant Professor, [2]PG Scholar
[1]Department of Computer Science and Engineering, [2]Dept. of Master of Computer Applications
Veltech Hightech Dr Rangarajan Dr Sakunthala Engineering College
Avadi, Chennai, India

ABSTRACT

Since the boom of smart phones and location-based services, spatio-temporal data (i.e., user locations with timestamps) have become increasingly essential in many real-life applications. To ensure these data are faithfully extracted from the underlying location tracking hardware and not altered by any malicious party or the user himself/herself, integrity assurance schemes such as digital signatures or message authentication codes (MAC) must be adopted. However, these conventional schemes disclose to the verifier the complete plaintext location and thus jeopardize users' privacy.

Propose an integrity assurance scheme with minimum location disclosure. That is, the granule of the disclosed location is just small enough to prove the user is/has been to a certain place, and the verifier cannot learn anything beyond it. To this end, a new MAC scheme called Prefix-verifiable MAC (PMAC), based on which we design indexes and protocols to authenticate both spatial and spatio-temporal predicates. Security analysis and experimental results show our scheme is both secure and efficient for practical use.

Keywords: *Location Tracking, Mobile Device, PMAC*

1. Introduction

Location-based services (LBS) have become increasingly popular in recent years, thanks to the intensive penetration of GPS-enabled smart phones and tablet computers. As more businesses and public services go mobile, spatiotemporal data (i.e., user locations with timestamps). The boom of smart phones brings prosperity to location- based services (LBSs) in almost all social and business sectors, such as geo-social networks, merchandizing, marketing, and logistics. Location-based services (LBSs) have been gaining tremendous popularity over the recent years, in particular since the emergence of mobile social networking services (mSNSs). Social networking giants such as Facebook and Twitter are all turning their services into mobile, along with specialized vendors like Foursquare, Gowalla and Loopt. The wealth of *space-time trajectories* left by these personal devices and their human companions is expected to enable novel classes of applications, for instance in traffic and sustainable mobility management, where the discovery of behavioral patterns is the key step. Internet technology with globally connected mobile networks introduces new business models and the development of service architecture. Location-Based Services (LBS) are such an example. Location based services (LBS) are Internet services that provide information or enable communication based on the location of users and/or resources at specific times. Service providers envision offering many new services based on a user's location as well as augmenting many existing services with location information.

The flourish of smart phones contributes prosperity to location based services (LBSs) in nearly all social and business sectors, such as geo-social networks, merchandizing, marketing, and logistics. A location-based advertisement and recommendation are often recognized as one of the most productive LBS businesses and thus provoke the greatest controversy with their ranking results, here it is examined the privacy-preserving authentication for location-based top-k queries, where the rank assess of an object is a linear compounding of distance penalty and non-spatial score (e.g., user average rating). This query resolution is like to an abstraction of several locations based top k queries defined in and even the k-nearest neighbour (kNN) querie.

1.1 Auditing and compliance

The location of a subject needs to be checked over time against some regulation.For example: a taxi should not leave its operating area designated in its license; a car rental requires the customer not to drive away from its service area for insurance coverage; a field engineer is supposed to visit a service site during working hours; and during a fishing or mining moratorium, a registered fishing vessel or a mining machine should not enter the region of moratorium.

Access control

Some businesses or services need to verify the user's geographic location before authorizing Access or providing services. For example: a mobile ad network gives away coupons of a shop only to those users who are visiting a shop of its competitors; an online casino must not accept customers from states where online gambling is illegal ; and an insurance

Testimony

A subject makes a claim of his/her historical location, which needs to be verified. For example, a passenger on a flight from a Zika-active country can waive further inspection by quarantine officers if there is a proof that he/she has not been to those outbreak zones.

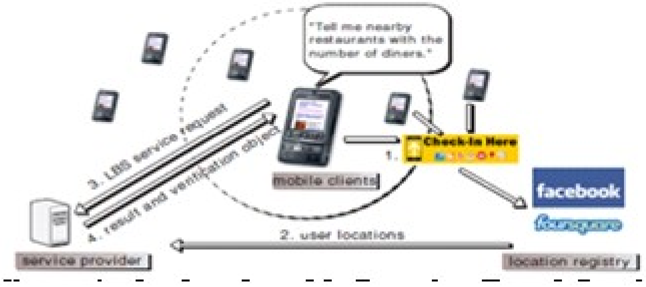


Fig **1. Authentic table Location-Based Service**

2. LITERATURE REVIEW :

2.1 Title: Mobile Client's Access Mechanism for Location based Service using Cell-ID

Description: Location Based Services (LBS) are information services that provide users with customized contents, such as the nearest restaurants/hotels/clinics, retrieved from a dedicated spatial database based on the user's current location. The LBS can obtain user's geographical position/location by making use of technologies such as Cell-ID, Global Positioning System (GPS), triangulation/triliteration etc. LBS not only serve individual mobile users, but also play important role in public safety. The role of Location Based Services is to retrieve the information directly related to the location of the user at the time of making the request.

2.2 Tittle: Proposed Authentication Model for Location Based Queries

Description: The concept of mix zones for the privacy of user's location, as aware application will have the potential to follow the user move. The security of the user is kept up constantly changing the username or pseudonym within some mix zone, but this does not provide full protection to the user's privacy. The concept of mix zones on road networks. This framework is to protect location privacy of mobile user's travelling on road network the new concept of Mob mix is also used to break up the continuity of user's location. The practical approach of this technique is difficult to achieve in practice. The concept of k-anonymity as a method for privacy preserving. By using generalization algorithm the concept of K-anonymity implemented, K-anonymity is a wide-spread general privacy concept not restricted to location privacy. It provides the guarantee that in a set of k objects (mobile users), the target object is non-identifiable from the other k – 1 objects.

2.3 Title: Research on Emergency Call and Location Tracking System with Enhanced Functionality for Android

Description: This system locates nearest available hospital, contacts its ambulance emergency system, accesses a Electronic Health Record of emergency patient that can critically assist in pre-hospital treatments. The system will identify availability of the nearest available specialized hospital all through EMS server which provides continuous information about the incoming patient to the hospital. This paper proposes Android Based Tracking for EMS (Emergency Medical System) on cloud. This system helps those sections of the people who unexpectedly fall into a situation where immediate communication of their situation becomes necessary to be informed to certain persons which will helps them in this condition. The proposed model is designed and implemented with the objective that it has to be user friendly and triggering of the application should take least time. The location of the user in problem should also be precisely known to all those persons whom message has been sent. This system is mainly deployed in an android-based phone that is conveniently used and carried. So this system is suitable for most of the people. With the help of the GPS and GSM network, the system can make sure the location of the users when they are in trouble and trigger the alarm.

2.4 TITLE: Location tracking using Google Cloud Messaging on Android

Description: Google Maps goes live. Just two months later, we add satellite view sand directions to the Product. Google Maps comes to mobile phones in the U.S. offering driving directions and local information to people on the go. Our first Google Maps release in Europe is geared to U.K. users. France, Germany, Italy and Spain follow in 2006. Today, we offer driving directions in 190+ countries around the world. Google Mobile Web Search is released, specially formulated for viewing search results on mobile phones. We unveil Google Earth, a satellite imagery-based mapping service that lets you take a virtual journey to any location in the world. Google Earth has since been downloaded more than 1 billion times. The Google Maps API is released; developers can embed Google Maps on many kinds of mapping services and sites.

3. RELATED WORKS:

3.1 The Location Privacy Protocols on Different Layers

This master thesis focuses on application layer protocols on location privacy; however we also looked at various works that approach the problem from different layers of the communication stack. There are some works that consider protection of the location privacy of users by focusing on physical layer. For example, there are use of RF finger printing, random silent period and Mixes in mobile communication systems , in order to protect location information of users from physical layer. Some other works approach from network layer. For instance, pseudonyms, mix zones and anonymous on demand routing are some of the works that aim to achieve the location privacy inside the network. The rest of this chapter is about related work on application layer.

3.2 The Location Privacy Protocols on Application Layer

Since one of the aims of this project is to investigate existing protocols on location privacy, the investigation started from K-anonymity. It has both strengths and weaknesses. For example, when a user is located in a crowd, K-anonymity can provide fast and simple solution. Since there are a lot of people around the user, it is very easy to form a cloaked region that users can hide underneath it. If the user is present in that area randomly, he/she can rely on K-anonymity. However, its weakness is the k value and working in a discrete and independent manner. Use of k value comes from a data mining point of view and it is not suitable for preserving location privacy most of the time. For example, an adversary might have knowledge about a user’s home and work locations.

3.3 Metrics for the Location Privacy

In which is an extensive analysis of existing protocols for the location privacy, later. Apart from K-anonymity, there are uncertainty-based metrics, clustering error based metrics and traceability based metrics. Shortcomings of existing location privacy mechanisms are explicitly shown in

4. PROPOSED MODEL:

Study the problem of spatio-temporal integrity assurance that incurs minimum location disclosure. Specifically, the disclosed granularity of the location is just precise enough to prove the spatio-temporal predicate is true, and the verifier learns nothing beyond this. Further, to support a wide range of (future) applications the integrity proof should not assume any predicate a priori. That is, a single proof, once generated, can authenticate the integrity against any upcoming predicates with variable region sizes and positions.

That addresses spatio-temporal integrity assurance in a privacy-preserving manner without wireless infrastructure or third-party witnesses. The problem is critical in database research community, and has wide applications in mobile computing industry. We design a prefix-verifiable message authentication code, based on which we develop authentication schemes for spatial and spatio-temporal predicates.We design two PMAC indexes and two optimization techniques that reduce the computation and communication costs.

4.1 LOCATION-BASED SERVICES

Location-based services are used to describe the different equipments used to find a device current location. Android provides access to the above elements to assist the performance of LBS services through the help of the four main LBS elements.

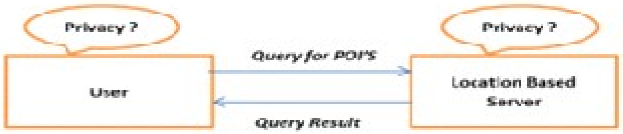


Fig **2. Location Based Service**

Location Manager: This element provides access to the location-based services. The following are some of the application of the location Manager.

- Obtain the current Location
- Track movement.
- Detect movement into and out of a specified area.

Location Providers: These represent different technology which are used to determine the device's current location or location-finding and provides periodic reports on the geographical location. It also determines the physical location, that is, handle GIS. , Location Provider component of Android application promote the resolution of the available provider(s) and the selection of suitable one among these available provider(s).

GPS gives the exact location of where we are standing .However in indoor situations GPS may not provide the location quickly.

Network location provider use mobile association provider and will give the adjacent tower location.

If the GPS is not enabled passive provider return coarse fixes.

Geocoding: Gooding can be done in two different ways. That is, reverse Gooding can forward geocoding. Conversion of geographical coordinates (longitude, latitude) into street address can be done using reverse geocoding whereas conversion of street address into geographical coordinates can be done using reverse geocoding. Reverse geocoding uses get Latitude () and get Longitude () to get the geographical coordinates.

4.2 GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATION)

Satellite foremost system that supplies location and time knowledge in all weather setting, throughout on or near the Earth where there is an open line of sight to four or more GPS satellites. The system offers important talents to military, polite and trade users around the world. It is allowed by the United States government and is freely nearby to anyone with a GPS receiver.

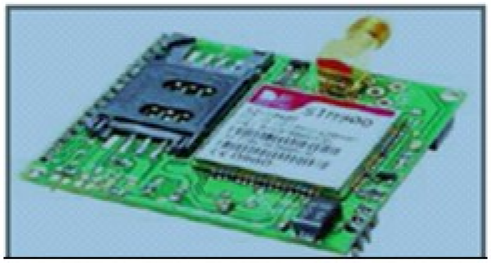


Fig **3. Global System for Global Communication**

GSM MODEM

GPS (GLOBAL POSITIONING SYSTEM)

The **Global Positioning System** (**GPS**) is a space-based satellite steering system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an open line of sight to four or more GPS satellites. The system provides critical capabilities to military, civil and trade users around the world. It is maintained by the United States government and is freely available to anyone with a GPS receiver.

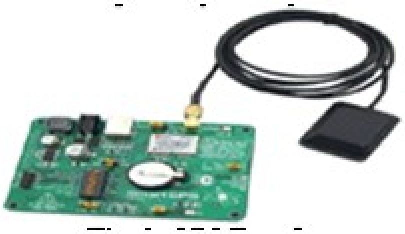


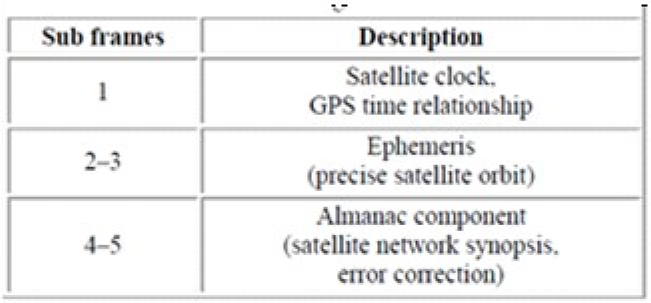
Fig **4. GPS BOARD**

CONCEPTS OF GPS (GLOBAL POSITIONING SYSTEM)

A GPS receiver estimates its place by exactly timing the signals sent by GPS satellites high above the Earth. Each satellite forever transmits messages that include

- The time the message was transmitted
- Satellite position at time of message transmission

The receiver uses the messages it receives to determine the transit time of each message and computes the distance to each satellite using the speed of light. Each of these lengths and satellites' locations defines a sphere. The receiver is on the surface of each of these spheres when the distances and the satellites' locations are correct.



Sub frames	Description
1	Satellite clock, GPS time relationship
2–3	Ephemeris (precise satellite orbit)
4–5	Almanac component (satellite network synopsis, error correction)

5. MODULES DESCRIPTION:

5.1 Find Persons: Find My Friends allows you to exchange REAL-TIME locations on Google maps with your Face book, Google+ and email friends. Location exchange is visible only to you and your selected friends. No report creation is necessary, the moment you start Find My Friends, you may directly trade locations with any of your friends WHO HAVE ALSO INSTALLED THE APP. You can also use Find My Friends to send constantly your location to close contacts (e.g. family members, spouse, good friends) even when you do not run the app. Moreover, you can set map zone and proximity alerts, and get notified when your friends enter / exit a map area and / or are nearby! Find My Friends also offers the "location to browser" extremely useful feature; If desired, you can transmit your REAL-TIME location to ANY online device with a web-browser

5.2 Track Location: The availability and fact of the Global Positioning System (GPS) offers increased abilities and safety for vehicles using highways, streets, and mass transit systems. Many of the problems associated with the routing and dispatch of commercial vehicles is significantly reduced or eliminated with the help of GPS. This is also true for the direction of mass transport systems, road maintenance crews, and emergency vehicles. GPS enables automatic vehicle location and in-vehicle navigation systems that are widely used through the world today. By blending GPS position technology with systems that can display geographic data or with systems that can automated convey data to display screens or computers, a new measure in surface moving is realized.

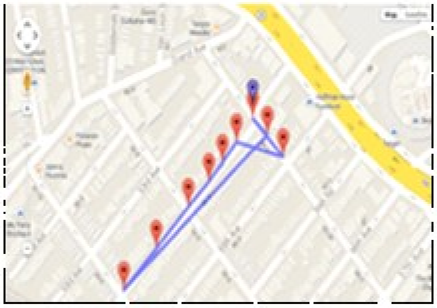


Fig 5. **Track Location**

5.3 Location Calculation: A user location is a where are the user's longitude and latitude, and t is the location timestamp. As coordinates and timestamps have finite precision in practice, assume they are all integers. The user needs to authenticate historical or current location to a verifier against some spatio-temporal predicates. According to a spatial predicate returns true or false about a relation between the user location and a spatial geometry. Focus on the containment predicate, i.e., whether the user "is" inside a rectangular window. A spatio-temporal predicate is augmented with a time interval, i.e., whether the user "has been" in this window. The meaning of "minimum location information" is twofold: 1) the user agrees to disclose to the verifier whether he/she is in the window or not; and 2) the verifier cannot learn anything about the user location beyond that.

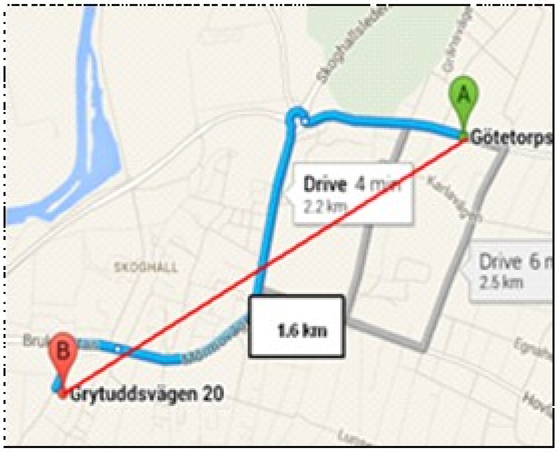


Fig **6. Location Calculation**

6. FUTURE ENHANCEMENT

As for future work, we plan to study the integrity assurance schemes for more complex predicates. In particular, we are interested in the complement of a containment predicate— a user is "not in" a specific region. This problem is even harder as it is equivalent to authenticating that a string x has a prefix from any of a set of strings, instead of all of them. Yet now we can manage limited number of users identity which is visualization of user location, this will be overcome by means of fetching separate server for gathering user's information by launching this, we can break the limitation which was occurred in previous task. So my future research will be able to implement the any number user's identity. And this any number of users information will also be grouped according to the nature of role they performing; it should be achieved by using filtering mechanism.

7. CONCLUSION:

We studied the problem of integrity assurance which discloses to the verifier no more information beyond the spatio-temporal predicate itself. The solution is based on prefix-verifiable MAC (PMAC), a cryptographic construct designed by us to verify the integrity of any prefix of a string. We then presented authentication protocols for both spatial and spatio-temporal predicates. Two indexing schemes for PMACs were proposed to pre-aggregate sub trajectories and accelerate the verification process. We further proposed two optimization techniques to reduce the computational and communication costs. Our security analysis and experimental results show that this authentication scheme is both secure and efficient for practical use.

REFERENCES

1. Amit Kushwaha, Vineet Kushwaha, "Location Based Services using Android Mobile Operating System", IJAET, Vol. 1,Issue 1,pp.14-20, Mar. 2011.
2. C. J. Shelke1, Ms. Grishma R. Bhokare "Location tracking using Google Cloud Messaging on Android" JARCCE, Vol. 4, Issue 12, December 2015..
3. R. Jegadeeswari 1, S. Parameswaran 2 "Location-Based Services Using Autonomous GPS", IJAET.
4. MihirGarude, NirmalHaldikar "Real Time Position Tracking System Using Google Maps", IJSRP Volume 4, Issue 9, September 2014
5. Ch.ChakradharaRao1, P.Pushpalatha2, N.AdityaSundar "GPS Based Vehicle Navigation System Using Google Maps",
6. Q. Chen, H. Hu, and J. Xu. Authenticating top-k queries in location-based services with confidentiality. In Proc. VLDB, 2014.
7. M.Graham and D. Gray. Protecting privacy and securing the gathering of location proofs – the secure location verification proof gathering protocol. In Proc. of 1st International Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec), 2009.
8. R. Hasan, R. Khan, S. Zawoad, and M. M. Haque. Woral: A witness oriented secure location provenance framework for mobile devices. IEEE Transactions on Emerging Topics in Computing, 2015.
9. H. Hu, J. Xu, Q. Chen, and Z. Yang. Authenticating locationbased services without compromising location privacy. In Proc. SIGMOD, pages 301–312, 2012.
10. C. Lyu, A. Pandea, X. O. Wang, J. Zhu, D. Gu, and P. Mohapatra. Clip: Continuous location integrity and provenance for mobile phones. In Proc. of IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, 2015.
11. A. Pham, K. Huguenin, I. Bilogrevic, and J. Hubaux. Secure and private proofs for location-based activity summaries in urban areas. In Proc. of ACM International Joint Conference on Pervasive and Ubiquitous Computing (Ubicomp), 2014.
12. S. Saroiu and A. Wolman. Enabling new mobile applications with location proofs. In Proc. of ACM HotMobile, 2009.
13. X. Wang, J. Zhu, A. Pande, A. Raghuramu, P. Mohapatra, T. Abdelzaher, and R. Ganti. Stamp: Ad hoc spatial-temporal provenance assurance for mobile users. In Proc. of 21st IEEE International Conference on Network Protocols (ICNP), 2013.
14. T. Xu and Y. Cai. Exploring historical location data for anonymity preservation in location-based services. In IEEE Infocom, Phoenix, Arizona, 2008.

15. Y. Yang, S. Papadopoulos, D. Papadias, and G. Kollios. Spatial outsoucing for location-based services. In Proc. ICDE, pages 1082– 1091, 2008.

16. Y. Yang, S. Papadopoulos, D. Papadias, and G. Kollios. Authenticated indexing for outsourced spatial databases. The VLDB Journal, 18(3):631–648, 2009.

17. L. Yap, T. Yashiro, M. Bessho, T. Usaka, M. Khan, N. Koshizuka, and K. Sakamura. Sucas: architecture for secure user centric attestation in location-based services. In Proc. of IEEE International Conference on Social Computing, pages 760–767, 2010.

18. Y. Zheng, L. Zhang, X. Xie, and W.-Y. Ma. Mining interesting locations and travel sequences from gps trajectories. In Proc.of International Conference on World Wild Web (WWW 2009), 2009.

19. Z. Zhu and G. Cao. Applaus: A privacy-preserving location proof updating system for location-based services. In Proc. of INFOCOM, 2011.

20. Z. Zhu and G. Cao. Toward privacy preserving and collusion resistance in a location proof updating system. IEEE Transactions on Mobile Computing, 2013.