A Comprehensive Study on Privacy Preserving Location Proof System

C.Subhashri[1] Dr.P.R.Vijayalakshmi[2]
[1]PG Scholor [2]Professor
[1,2]K.L.N.College of Engineering, Sivagangai

Abstract— In recent years, location based mobile devices has an important aspect. Mobile device users can access many applications through servers based on their current locations. It is a challenge to prove their presence at a specific location in a secure and privacy protected approach. Location privacy is obligatory to each and every user to keep their location confidential. In this paper, we have presented a comprehensive study about the various methods that are well suited to protect location privacy and location proofs.

Key words: location proof, location privacy, localization methods, anonymity

I. INTRODUCTION

As location based mobile device are immensely growth. Most of the technique based on the current locations. Users find their current location and send it to the server and the server provides the resources to the user based on the current locations. It is challenge to find the users geographical locations. Saroiu et al explained several applications in [1] that are(1) A general problem on auction websites as ebay is account theft- attackers break into valid accounts and use their customary reputations to commit fraud.(2)Many police investigations are quickly resolved by tentative the alibis of the persons involved in an incident. With location proofs, people can use their mobile phones to make such alibis.(3) During an election, voters are frequently asked to provide proof of their existence in particular region, state or country for a pre-determined period of time.

The above applications need users to be able to obtain proofs from the locations they stopover .Users may then choose to present one or more of their proofs to a third-party verifier to claim their existence at a location at a specific time. Geo-location data is collected in many ways, including Global Positioning System devices, IP address, or Wi-Fi network mapping. Location proof plays a very important role in location based applications. Location proof is a piece of data that certifies spatial and temporal information about the mobile device of the users. In the location proof updating system, location information is able to be stolen by adversaries. It may cause exposure towards location privacy of the user. Public key Cryptographic technique is used for encryption and decryption of communicating messages and secure from eavesdropping.
The important issues and design challenges involved. They are,

A. Security:

The security of location proofs are two properties: *integrity* and *non-transferability.*

The integrity property requires that no user can create fake location proofs by himself/herself .

The non-transferability property requires that no user can claim the ownership of another user's legitimate STP proofs.

B. Privacy:

1) Anonymity:

Location privacy is the more important factor that needs to be taken into concern when designing any location based systems. First, a user should be able to hide his/her identity from another user.

II. RELATED WORK

Different techniques are involved on privacy preserving technique towards location proof. Each and every technique is having its own functionality. There are,

A. A WiFi-Coverage Based Location Verification System in LBS:

The aim of the paper is to design a novel verification system named WILOVE. It maps the physical area of a venue to the local WIFI coverage and involves the venue owner as the verifier and also to design an adaptive algorithm for preserve against proxy attacks based on the check-in delay.

1) Design of WILOVE:

Design process involve the venue owner as a local verifier, the system architecture transforms from a client-server structure in LBS system to the trilateral one in WILOVE.

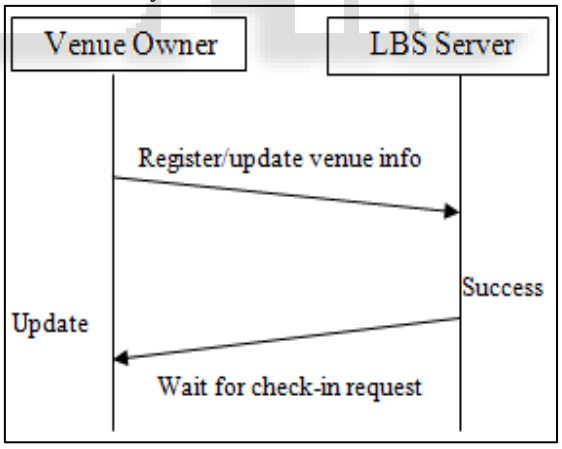

Fig. 1: Flow between venue owner and LBS Server

The user operates through a smart phone while the verifier can use either a mobile device or a computer connected to local WiFi access point (AP).

1. The user and the verifier each produce an asymmetric key-pair, all the communications are encrypted using these keys. The server acts as a trusted entity to distribute public keys between them.2. The verifier's WiFi SSID and IP address are integrated in the venue info and updated to the server.3. The user can acquire the SSID and IP of the verifier from the server, and now it sends check-in requests to the verifier instead of the server; the verifier notes on a predefined port for the check-in requests. 4. The

All rights reserved by *www.ijsrd.com*

verifier verifies the user with encrypted messages which are dynamically generated.5. The time spent on the message decryption and communication during the verification is working to detect proxy attack.

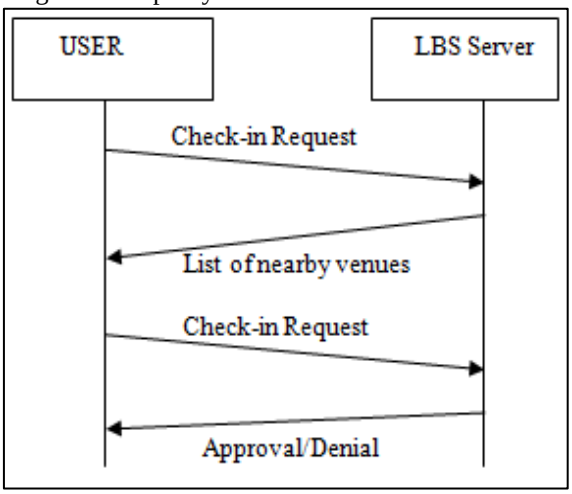

Fig. 2: Flow between User and LBS Server

2) Disadvantage:

1.The system have strong needs of check-in security.

B. Location Tracking using Google Geolocation API:

The main aim of this paper is to track the location of the user with the help of Google API and to obtain the current geographical position of the hosting device or the user.

1) Methodology:

The designed system used for obtaining the current location of the user. The block diagram of the proposed system is,

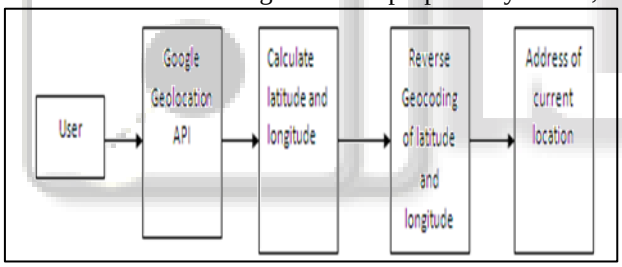

Fig. 3: Block Diagram of Location Tracking

2) Geographic Coordinates Calculation:

In this step to calculate the Geographic coordinates i.e. latitude and longitude of the present location the geographical coordinates will be got with the help of Geolocation API. getCurrentPosition ( ) method find the current geographic location of the user . The location is articulated in terms of geographic coordinates i.e. latitude and longitude.

var lat = position.coords.latitude;

var lng = position.coords.longitude;

3) Reverse Geocoding:

Reverse Geocoding is the scheme of reverse coding of a location having geographical coordinates i.e. latitude and longitude to a readable address. This allows the identification of close by street address, places, and subdivisions such as neighborhood, county, state.

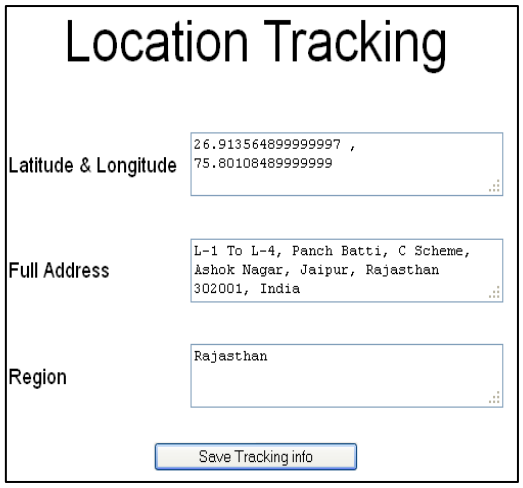

Fig. 4: Method of track the Location

4) Disadvantages:

1) This system does not work if geolocation API is down due to some reason.
2) It cannot find out the past location of the user.
3) It finds out only the approximate location.

C. Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System:

The main aim of this paper is to design A Privacy-Preserving LocAtion proof Updating System (APPLAUS) which is used to mutually generate location proofs and also increase user-centric location privacy model in which individual

Method of location tracking users evaluate their location privacy levels.

1) Location proof updating system:

In APPLAUS, mobile nodes communicate with neighboring nodes with Bluetooth, and communicate with the untrusted server through the cellular network interface.

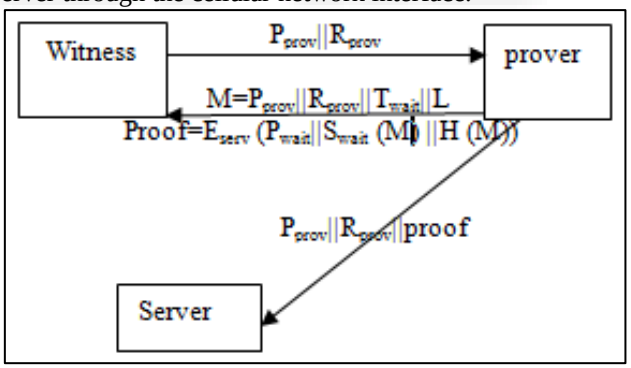

Fig. 5: Flow of location proof updating system

2) Collusion Detection:

here are two approaches to detect suspicious location proofs and pseudonyms

3) betweenness ranking:

This approach calculates the betweenness of each pseudonym in a graph and then position these pseudonyms based on their betweenness value. The pseudonyms with short ranking are considered as suspicious nodes.

4) correlation clustering:

This approach takes with the time delay between two neighboring location proofs, and uses a personalized correlation clustering algorithm on a temporal-weighted graph to rule out outlier clusters, which are considered as suspicious location proofs.

All rights reserved by www.ijsrd.com

5) Disadvantages:

1) In this method takes more time consumption.
2) It can only find out the current location not the past location.

D. Location Proof via Passive RFID Tags:

The main aim of this paper is to introduce two protocols that provide secure and accurate location proof service with passive RFID tags and this paper presents a solution to derive users' real time of existence in the absence of a reliable clock.

1) Methodology:

There are two protocols anticipated for two different situations. The first one utilizes a server (one can communicate with it using cellular communication, for instance), while the other requires no real time interaction from any devices other than the passive RFID tags.

2) Online protocol:

Online protocol assumes the availability of a remote server to provide real time information that aids the local tags in given that the location proof service.

Flows:

```
Flows:

R to S    : Location Proof Service Request
S         : creates a new session for R;  generates r;
            records r,t
S to R    : r, t
R to Tid  : r
Tid       : computes h(r, Sid)
Tid to R  : h(r, Sid), Tid
R to S    : h(r, Sid), Tid, {Tid}R
  S       : verifies h(r,Sid); create the location
Proof     : {Tid, {Tid}R, t}Server ; end session
S to R    : {Tid, {Tid}R, t}Server
```

Fig. 6: Flow of Online Protocol

3) Offline Protocol:

Offline protocol that is not relies on real-time server interaction with the user. The server can be contacted at some time after users' supply timestamps to the RFID tag to provide the users to with their location proof.

The protocol contains two major components. The first component is exclusively between the reader and the tags, carried out locally in actual time. The second component can be carried out at a later time, and is exclusively between the reader and the server.

```
Flows:

R to Tid          : t
Tid computes      : v=h(t,n,Sid), n++
Tid to R          : v,n,Tid

R and S           : exchange a challenge-
response

                  : nonce N to verify R's ID
R to S            : v, n, Tid, PKR, t
S verifies        : v == h(t, n, Sid)
S calculates      : ^t
```

Fig. 7: Flow of Offline Protocol

4) Disadvantages:

1) The protocol needs to address denial of service attacks.
2) The efficiency of the protocol is low compare to other methods.

E. Privacy Preserving Scheme for Location-Based Services:

The main aim of this paper is to build a fully secure system that allows users to promote from location-based services while preserving the confidentiality and integrity of their data and also to allow an executor (*i.e.* LBS server) to receive encrypted inputs/requests and then execute a blind search to retrieve encrypted records that match the selection criterion.

1) Homomorphic encryption schemes

It allows performing arithmetic operations (additions and multiplications) above encrypted data, meaning that the effect of an arithmetic operation would be the same whether applied over plain bits or encrypted bits.

In this system, processing a user's demand goes through the following four main steps:

1) Localizing category
2) Localizing services
3) Filtering services

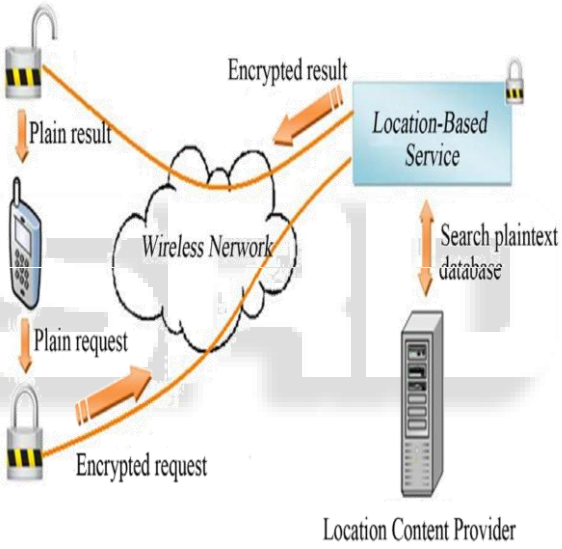

Fig.2.7.Architecture of secure location based service

2) Disadvantages:

1) If large number of services involved the performance is low.
2) The number of operations increases, while the number of records supported gets lesser.

F. STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users:

The main aim of this paper is to find the past location of the mobile users in efficient and secure manner. For this purpose to design Spatial Temporal provenance Assurance with Mutual Proof(STAMP) for ad-hoc mobile users for generating location proof and guard users against collusion using a light-weight entropy-based trust evaluation approach.

1) STAMP Scheme:

STAMP scheme is used to generate the spatial Temporal Provenance(STP) Proof and used to claim the STP proof and perform verification process.

2) Distance Bounding:

A location proof system needs a prover to be securely localized by the party who provides proofs. A distance

All rights reserved by www.ijsrd.com

bounding protocol serves the purpose. Proposed system used Bussard-Bagga as a Distance Bounding protocol.

3) Zero Knowledge Proof:

It is a method by which one party (the *prover*) can prove to another party (the *verifier*) that a given statement is true, without assigning any information apart from the truth that the statement is indeed true.

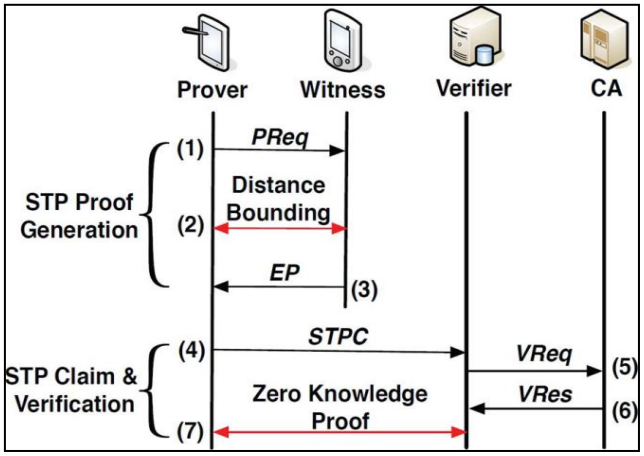

Fig. 8: STAMP Protocol

4) P-W Collusion Detection:

To detect P-W collusion entropy-based trust model is used. It measures the likelihood of such an attack. The trust evaluation is done by CA, which requires CA to keep track of the STP proof transaction history between any two users.

A user's STP proof transactions include both the STP proofs he/she gets as a prover and the STP proofs he/she creates as a witness.

III. Conclusion

This paper compares many location based services methods and also highlighted the demerits of each and every method. This comprehensive study concludes that to find the past location without harming the user's privacy is one of the challenges. From this survey STAMP method provides enough privacy property with finding the past location and also avoid from the collusion. So it provides the location proof effectively and defense against proxy attack and also replay attack.

References

[1] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in Proc. ACM HotMobile Art. no. 3,2009

[2] Yifan Zhang; Chiu C. Tan; Fengyuan Xu; Hao Han; Qun Li, " VProof: Lightweight Privacy-Preserving Vehicle Location Proofs",IEEE Transactions on Vehicular Technology, Volume: 64,Pages: 378 – 385,2015

[3] Monika Sharma,Sudha Morwal, "Location Tracking using Google Geolocation API"IJSTE, Volume : 1,pages: 29-32,2015

[4] Ruben Rios,Jorge Cuellar, Javier Lopez , "Probabilistic receiver-location privacy protection in wireless sensor networks",Elsevier,Information sciences, Volume: 321,pages: 205-223 ,2015

[5] Xin ye Lin,Wenbo He, " WiLoVe: A WiFi-Coverage Based Location Verification System in LBS",Science Direct,International Conference on Mobile Systems and Pervasive Computing,Volume: 34,pages: 484-491,2014

[6] Zhichao Zhu,Guohong Cao, "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System",IEEE Transactions On Mobile Computing,Volume: 12, Pages 51-64, 2013

[7] Shawn Merrill , Nilgun Basalp , Joachim Biskup, Erik Buchmann, Chris Clifton, Bart Kuijpersk , Walied Othman, Erkay Savas, " Privacy through Uncertainty in Location-Based Services", IEEE International Conference on Mobile Data Management, Volume: 2,Pages: 67 - 72,,2013.

[8] Harry Gao, Robert Michael Lewis, Qun Li, " Location Proof via Passive RFID Tags"Springer,Wireless Algorithms, Systems, and Applications, Volume:7405, pp 500-511,2012.

[9] Jindan Zhu,Kai Zeng,Kyu-Han Kim,Prasant Mohapatra, " Improving Crowd-Sourced Wi-Fi Localization Systems using Bluetooth Beacons",IEEE Communications Society Conference, Pages: 290 – 298,2012

[10] Youssef Gahi ,Mouhcine Guennoun, Zouhair Guennoun, Khalil El-Khatib, " Privacy Preserving Scheme for Location-Based Services",Springer Journal of Information Security,Volume: 3,PP: 105-112, 2012.

[11] Ioannis Krontiris,Felix C. Freiling,Tassos Dimitriou," Location Privacy in Urban Sensing Networks:Research Challenges and Directions",IEEE Wireless communication,Volume: 17, Issue: 5,Pages: 30 – 35,2010.

[12] X. Wang et al., "STAMP: Ad hoc spatial-temporal provenance assurance for mobile users," in Proc. IEEE ICNP , pp. 1–10, 2013.

[13] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudonymity-a proposal for terminology," in Designing Privacy Enhancing Technologies. New York, NY, USA: Springer, 2001.

[14] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 370–380, Feb. 2006.

[15] S. Halevi and S. Micali, "Practical and provably-secure commitment schemes from collision-free hashing," in Proc. CRYPTO, , pp.201–215, 1996.

[16] I. Damgård, "Commitment schemes and zero-knowledge protocols,"in Proc. Lectures Data Security, pp. 63–86, 1999.

[17] I. Haitner and O. Reingold, "Statistically-hiding commitment from any one-way function," in Proc. ACM Symp. Theory Comput., pp.1–10, 2007,.

[18] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in Proc. IEEE MASS, 2005.

[19] J. Reid, J. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in Proc. ACM ASIACCS, pp. 204–213,2007,.

[20] C. Kim, G. Avoine, F. Koeune, F. Standaert, and O. Pereira, "The Swiss-knife RFID distance bounding protocol," in Proc. ICISC, pp. 98–115, 2009.

[21] H. Han et al., "Senspeed: Sensing driving conditions to estimate vehicle speed in urban environments," in Proc. IEEE INFOCOM, pp. 727–735,Apr.2014,.

All rights reserved by www.ijsrd.com