PRIVACY-PRESERVING LOCATION PROOFS USING CENTRALIZED DECENTRALIZED SYSTEM

Krutika Thakur [1], Laxmi Bewoor [2]

1Department of Computer Engineering, Vishwakarma Institute of Information Technology,Pune,India

2Department of Computer Engineering, Vishwakarma Institute of Information Technology,Pune,India

ABSTRACT

Nowadays location based services area unit quickly turning into common. Several services that area unit supported users location can even use the users location history or their spatial temporal place of origin. It uses GPS technology international Positioning System (GPS) could be a satellite-based navigation system created of a network of various satellite. Malicious users could slug their spatial-temporal place of origin while not strictly represent security for users to prove their past location proofs. Basically the system is design for mobile users. The system must be generate location evidences for each users who are connected in network. Users can share their proof in centralized as well as decentralized manner. Therefore it can be acceptable for trusted user and access points which are in network. Certification Authority is uses to divides cryptographic keys which are uses for authentication purpose which opposes collusion .The implementation is on android platform i.e low cost in terms of storage resourses . Scheme should be entropy based which main purpose is to detect users fake proofs.

Keywords : Global Positioning System, Location Proof, Privacy, Spatial-Temporal beginning

I.INTRODUCTION

Location in geography are uses to identify a point or an area on the earth or elsewhere. Nowadays we mostly uses locations in mobile phones which uses for detect present location. Location based services are mostly software level that uses for location data .Location based services are like maps and navigation, tracking services, information services and application like social networking.

Location base services is standardize concept of real time locating systems. The most useful services is detecting location by using mobile devices. The services are like users can discover or find their location and also they can share that information with server. After getting the information server performs mathematical or computation based on t location information and it returns data related to it as well as provide services to the users. Most of these days several location based services think about users i.e location which is supported to their devices by GPS. By using ”latitude” and ”longitude” it allow a users to track known persons location in day to day time.

Location based social networking is one of the application of an location based service in which person can share location proof with the server. And after that server accepts the request only when the sender is represent a true evidence of location. Mostly cellular service devices are uses for generate proofs and tracking that services can helpful certify the locations of mobile users in day to day time. Location based services think about users location supported their devices exploitation GPS. It permits some malicious users to faux their atm info. so there’s have to be compelled to accomplish integrity of atm proofs. essentially atm stands for abstraction Temporal root wherever abstraction suggests that one thing concerning area, Temporal suggests that one thing concerning time and last however not the smallest amount root is expounded to history of one thing. Location based services are uses STP which stands for spatial temporal provenance. The meaning of STP is something related to space and time and the provenance is nothing but history of something. Because of location based services allow malicious uses to fake their provenance information ,therefor there is need to achieve integrity of evidence.

II.REVIEW OF LITERATURE

Xinlei Wang [1] author detect the present as well as past location of a mobile user by using the spatial temporal information of particular user. And also it provide an digital proof of it. Spatial temporal aim of security for users to proving past locations .They uses STAMP scheme and it developed for mobile users who generate the location proofs for each other distribute manner. Also they uses cryptographic keys for avoid collusion.

Stefan Saroiu [2] this paper introduce location proof is nothing but an mechanism which generates proofs. They uses fields like issuer, recipient, geographical location and a digital signature. Also they uses ”latitude” and ”longitude” to define the location. In it also uses the public key to verify integrity of location proof. They proposed system which has four security properties like integrity, non-transferability, unforgeability, privacy.

Chien-Ming Chen [3] propose a condition-based location authentication protocol for mobile devices to authenticate users location claims. This protocol collaborates with other
neighboring mobile devices to generate the trusted proofs. This protocol does not require any extra equipment built in mobile devices, thus, it is easy to use and deploy.

Zhichao Zhu [4] Author proposes a system in which they uses location based services that mostly depend on mobile devices to determine location it sends to the application. In this system bluetooth enabled mobile devices generate location proofs and update that proofs to server. They also develop centric location privacy model in which users evalute their location in day to day life.

Ragib Hasan [5] In this paper the author represent a scheme with relies on location proofs from multiple wireless access points from Bluetooth enabled mobiles which is in peers. So that no user can parden the proofs without colluding. In this mobile user certifies his position before obtain access to the resources. Here they solve the issue like compution communication in private manner.

III.OBJECTIVES

i Integrity : - It is nothing but assurance that information is trustworthy and accurate.information must be taken to ensure that data con not be altered by unauthorized peoples.

ii non-transferability: - It nothing but not able to be transferred to another person. It is designed verifier proofs .Once a location proof is supplied, it cannot be transferred from one user to another.

iii Protecting users privacy : - It is use for reduce the privacy risks and it deal with ability an organization or individual that to determine what data in a computer system can be shared with third parties.

iv .Location-proof based mobile applications : - Design with objective of protecting users anonymity in which network enables user to admit the web and in that monitoring is important. Also it prevent traffic analysis and location privacy.

IV.SYSTEM OVERVIEW

i Problem Statement

In order to provide secure technique that detect the location of user who sometimes user say untruth about their location thus we cannot depend on the users devices to discover and transmit location information because users have an incentive to cheat, thus developing system in which it detect the present as well as past location of particular user.

V.FIGURES

System Architecture

The Fig. 1 shows the proposed system architecture. We develop a system in which an STP proof scheme are important. It is related to the spatial and temporal proofs i.e it requires space and time for generate evidences. It main goal are provide the truthfulness and non-transferability of proofs ,also with capability of protecting privacy. It requires an access point to create proofs for mobile users.

There are four sorts of modules

- Prover
- Witness
- Verifier
- Certificate Authority (CA)

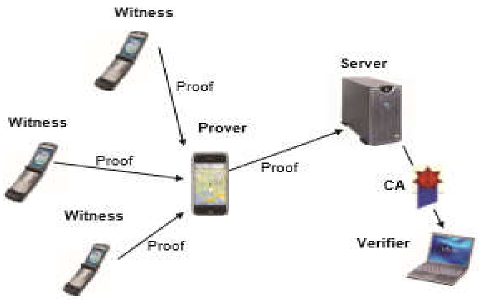

Fig. 1. System Architecture[1]

1) Prover: A prover a mobile device mobile which tries to obtain evidences at a particular location. The prover stores all location proofs which is collected on a mobile devices under his control to use them at a later time.

2) Witness: A witness is a device that connectivity with the prover in one network and it is willing to form an standard proof for the prover by receiving its request. The witness may be untrusted or trusted. Witness will be mobile or wireless Access points . The identity of a witness must be kept secret from the other users of the system, with the exception of the anonymity.

3) Verifier: A verifier is the party that prover needs to point out one or a lot of standard evidences to and claim its presence at a location at a specific time. This role play publicly lie in bank, store ,police authority etc

4) Certificate Authority (CA): This a trusted third party responsible for issuing the credentials to newly registered users. This authority is only used to register new users and is not involved in the generation of location proof.

In architecture, prover should be a mobile device or handset and witness must be mobile handset or wireless access points and they communicate with each other through bluetooth or wifi in network. In this scheme proof generation system is there for prover and therefore it presents list of multiple resources i.e witnesses. There are multiple witnesses are their and they eager to collaborate with mobile devices of prover and then prover start to collaborate with witness sequentially. The evidences claims are send to verifier periodically from prover i.e mobile device through internet or LAN. And this system we conclude that verifier having internet connection with trusted party. In this system multiple usre's are their and they can act like prover or witness. The role should be depend on their moment Sometimes users must be a witness and the witness must be work as user. The system must be assume that there is having identification of an user and they have one public key which is verify by trusted party i.e CA. Each user who connected in network have unique public key and that is generates when the registration process is their. After registration done the key is stores in with user's personal devices.

ii. System Scheme

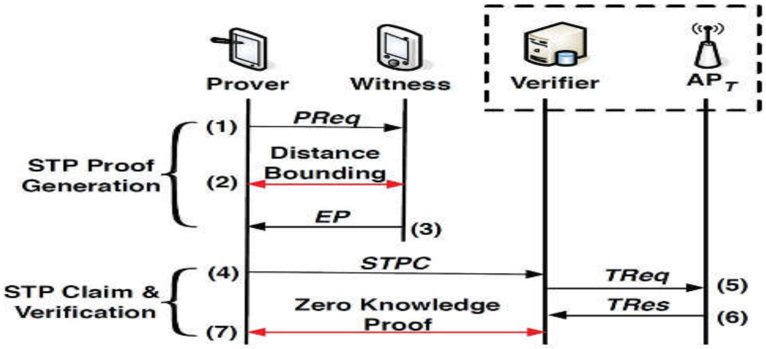

Fig 2. An illustration of System Procedure

A) Preliminaries

1) Location Granularity Levels:

We assume there are granularity *n* levels for each location, which can be denoted by L1,L2…Ln , where L1 represents the finest location and Ln the most coarse location granularity.

2) Distance Bounding :

A location proof system needs a prover to be securely localized by the party who provides proofs. A distance bounding protocol serves the purpose. A distance bounding protocol is used for a party to securely verify that another party is within a certain distance.

The type of distance bounding is a most popular category is based on fast-bit-exchange : one party sends a challenge bit and another party replies with a response bit and vice versa. By measuring the round-trip time between the challenge and the response, an upper bound on the distance between the two parties can be calculated. This fast-bit-exchange phase is usually repeated a number of times.

The Bussard-Bagga protocol proposed in [9] is based on a zero-knowledge proof technique, and it allows the prover to be authenticated via a private/public key pair. Hence, we adopt the Bussard-Bagga protocol as our distance bounding protocol. The protocol consists of three stages. The first stage is the preparation stage, where the prover encrypts his/her private key K^{-}_{p} with a random symmetric key and gets an encrypted message *e.*

B) Protocol :

i) Overview :

Protocol consists of two primary phases: STP proof generation and STP claim and verification. Fig. 2 gives an overview of the two phases and the major communication steps involved.

When a prover collects STP proofs from his/her co-located mobile devices, we, an STP proof collection event is started by the prover. An STP proof generation phase is the process of the prover getting an STP proof from one witness. Therefore, an STP proof collection event may consist of multiple STP proof generations. The prover finally stores the STP proofs he/she collected in the mobile device.

When a prover encounters a verifier and he/she intends to make a claim about his/her past STP to the verifier ,the STP claim and verification phase takes place between the prover and the verifier. A part of the verification job has to be done by CA. Therefore ,communication between the verifier and CA happens in the middle of the STP claim and verification phase.

ii) Collusion Detection: If a prover colludes with a witness, it is easy for the witness to give the prover a legitimate STP proof with fake spatial-temporal information. Since the STP proof generation process is done in an opportunistic manner and we do not assume a trusted party in this process, a P-W collusion cannot be prevented or detected with a 100% certainty. As a counter measure against P-W collusions, here proposed an entropy-based trust model which 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.

VI.CONCLUSION

In the Proposed system to produce security and privacy to mobile users evidences for his or her past location visits. System depends on mobile devices therefore generating location proofs continuously to server. Integrity and non-transferability are the main objective of system to provide location proofs and privacy of users**.**

VII.ACKNOWLEDGMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are thankful to the authorities of Savitribai Phule University,Pune and concern members of ICETSET conference, organized by, for their constant guidelines and support. We are also thankful to the reviewer for their valuable suggestions.

REFERENCES

1] Xinlei Wang, Amit Pande, Jindan and Prasant Mohaptra, STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users,IEEE Trans. On Networking,Jan 2016.

[2] Saroiu and A. Wolman, Enabling new mobile applications with location proofs, in Proc. ACM HotMobile, 2009.

[3] Chien-Ming Chen; Xiaojie Zhang; Tsu-Yang Wu A Secure ConditionBased Location Authentication Protocol for Mobile Devices 2016

[4] Z. Zhu and G. Cao, Towards privacypreserving and colluding-resistance in location proof updating system, IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 5164, Jan. 2011.

[5] R.HasanandR.Burns,Wherehaveyoubeen?securelocationprovenance for mobile devices, CoRR,2011.

[6] Zhichao Zhu and Guohong Cao,APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services IEEE Transactions on Wireless Communications

[7] I. Krontiris, F. Freiling, and T. Dimitriou, Location privacy in urban sensing networks: Research challenges and directions, IEEE Wireless,2010.

[8] Chitra Javali, Girish Revadigar, I Am Alice, I Was in Wonderland: Secure Location Proof Generation and Verication Protocol

[9] Youssef Gahi, Privacy Preserving Scheme for Location-Based Services Journal of Information Security, 2012

[10] N. Sastry, U. Shankar, and D. Wagner, Secure verification of location claims, in Proc. ACM WiSe, 2003, pp. 110.