ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

A Survey on Preserving Privacy towards Location Proof

Senthilguru S, Blessed prince P

Abstract— 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.

***Index Terms*— anonymity, location proof, location privacy, localization techniques.**

.

I. INTRODUCTION

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 [5][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 [10]. 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. To obtain the location privacy mobile nodes are expected to satisfy some or all of the basic properties given below: [11]

***Location privacy*:** It is defined as an ability to prevent the unauthorized entities to access the location data of current and past locations.

Senthilguru S,PG Student, Information technology, Karunya University , Coimbatore, India
Blessed prince P, Assistant Professor, Information technology, Karunya University , Coimbatore, India

***Identity privacy*:** Mobile node is not able to find the identity of the user, based on the location information received during the location proof request .The real identity of the user should not be traced by the malicious node known as untraceability.

***Unlinkability*:** No unauthorized entity should be able to relate different sessions of the mobile node.

Depending on the scope, nature, and behavior of attacks, the attackers can be classified as follows: [2]

- Passive attackers participate in eavesdropping messages in communication.
- Active attackers will not forward the received packet to its destination by dropping or it may generate packet containing immoral information.
- Inside attacker are the authentic members of the network, sometimes it acts as the adversary.
- Outside attackers are the intruders.
- Malicious attackers are not getting any benefit personally by their attack. Their aim is to harm other members of the network or disrupt the functionality of a MANET.
- Local attacker attacks up to the limited radio range. An attack can be extended, where an attacker organized as a group across the network

II CHALLENGES IN MOBILE NETWORKS

A. Insecure Boundaries

There is no clear secure boundary in the mobile ad hoc network, when compared with the defense available in the traditional wired network. This vulnerability originates because of its nature that gives the freedom to join, leave and move inside the network.

B. Restricted Power Supply

Due to the mobility of nodes in the ad hoc network, it is common that the nodes in the mobile ad hoc network will rely on battery as their power supply method. The restricted power supply may lead to denial-of-service attacks. Moreover, a node in the mobile ad hoc network may behave in a selfish manner when it finds that there is only limited power supply, and the selfishness can cause some problems when there is a need for this node to assist with other nodes to support some functions in the network.

C. Scalability

As the nodes are mobile, the scale of the Mobile ad hoc network keeps changing all the time. It makes it tough to predict how many nodes will be in the network in the future. As a result, the protocols and services that are applied to the mobile network should be compatible to the continuously changing scale of the ad hoc network.

III DIFFERENT TECHNIQUES ON PRIVACY PRESERVING TECHNIQUE TOWARDS LOCATION PROOF

A. Location Privacy in Pervasive Computing

Location privacy is a particular type of information privacy that we define as the aptitude to prevent other parties from learning one's current or past location [4]. With pervasive computing, though, the scale of the problem changes entirely. Most likely you do not care if someone finds out where you were yesterday at a particular time, but if this someone could look over the history of all your past movements, recorded every second with sub meter precision, everyone might start to see things differently. Then they focus on the privacy aspect of using location information in pervasive computing applications. They do not essentially need to stop all access because some applications can use this information to provide useful services. But, we want to be in control and to keep our position secret but wanting social group to be able to locate us with privacy. So they build Privacy-protecting framework based on frequently changing pseudonyms. So users avoid being identified by the locations they visit [7]. In that they introduce the concept of mix zones and showing how to plot the problem of location privacy onto that of anonymous communication. Pseudonym is used to destroy the link between location information and user identity. Untraceability, by itself, may not be enough in pseudonym based approach. The provision of unlinkability is related to an aspect of privacy also referred as path privacy. Adversary has no coverage in silent mix zone [8]**.**Multiple pseudonyms for unlinkability prevent from correlation attacks.

Demerits:

- Global eavesdropper can monitor the network by traffic analysis techniques.
- Designed with increasing complexity of user registration and computational storage and communication cost.
- To obtain path privacy a user might have to update a pseudonym at points where the spatial and temporal resolution is decreased e.g., inside a mix zone.

B. Wi-Fi Access Points Issuing Location Proof

Location proof of mobile node contains five fields: proof issuer, proof recipient, timestamp, geographical location, digital signature. In this case proof issuer is Wi-Fi access point. Wi-Fi access points (AP) advertise its presence by broadcasting beacon signals to its surrounding area [5]. If the recipient needs the location proof then it extracts the beacon's sequence number and uses it for asking the location proof. The demand for a location proof contains the client's public key and the signed AP's sequence number. The client signs the sequence number to guard their reliability and to make it hard for others to masquerade as client devices. Then AP checks whether the signature is legitimate and whether the sequence number is current one. If the request is valid, the AP creates a location proof with a current timestamp and designates to the client. If the request is invalid then AP drops the request mutely. Another sensible consideration is making sure that APs are configured with the correct location coordinates. While it is cheap to provision APs with GPS to routinely determine their geo-location, most APs are situated in indoor environments where GPS does not work fine. One way to overcome this complexity is to provide the AP with an additional configuration interface for administrators. To point a location proof-enable AP, the administrator initially takes the AP outdoors and runs a setup program that uses GPS to establish the AP's location

Demerits:

- Proof issuer will not know whether the recipient received location proof or not.
- Denial-of-service attack is performed by the recipient, so the computational resources may be degraded to AP or issuer.
- Access point may be relocated then it must be reconfigured to the new longitude and latitude to provide the valid location proof to requester.

C. Proving Your Location without Giving Up Your Privacy

A location proof is an electronic form of article that certifies someone's bearing at a definite location at particular time [10]. A retroactive location proof is used to currently interact with a target application. A proactive location proof is collected for the future purpose, without having a goal application in mind. Cryptographic hashes and digital signatures are used for user anonymity. Location proof request is sent to the AP by the user, with granularity. If AP receives the request it generates nonce for itself and then sends the nonce to the user. Then user concatenates the received nonce with user nonce and signs them. At last AP creates a location proof which is enclosed by group signature which is finally send to user. The issuer gets the hash of the signature and its nonce. The hash in combination with the user's nonce serves for two purposes: First, they behave as a commitment by the user to her signature. Finally, it hides the user's signature and therefore his identity from the proof issuer. A dishonest user may collude with a malicious intruder. This is to launch a replay attack to acquire location proofs for a place where the dishonest user is no longer located. The task of the malicious intruder is to acquire further location proofs from the same proof issuer on behalf of the dishonest user, who is moved away. It's impossible for malicious intruder to succeed, that the proof issuer is going to re-use nonce. However, since each nonce is used only once, the malicious intruder cannot thrive.

Demerits:

- It is impossible to sign the fresh nonce by the malicious intruder but he may try to set up a communication channel through which he can send a fresh nonce to the remote dishonest user to include his signature with the nonce in real time by wormhole attack.

D. Customizable K-Anonymity Model

Personality identifiable information is being openly unknown as anonymity. Customizability means user can

flexibly control the tradeoff between privacy protection and accuracy for LBS [13]. Customizable k-anonymity model for protecting privacy of location data works by, thrashing the location of a user within a cluster of k members. A third party is employed to gather the user's locations and classify them in some k-size sets. Then one of the members of the location set is chosen as the representative location of all those users. k-anonymity approach utilizes a trusted third party as an anonymizer, where the implementation could be based on a centralized or distributed architecture. The vital challenges in k-anonymity are to come across k-1 other users to keep the anonymity. Two other evils with k-anonymity approach are the reduction of accuracy and they require for a trusted third party.

Demerits:

- It depends on trusted third party
- In this case Location privacy is inversely proportions to location accuracy

E. Event Source Unobservability.

An adversary has same credentials as legitimate mobile user. So the real event source can be eavesdropped by the adversary [9]. The local adversary and global adversary can analyze the traffic, to find what information is passed by the user by traffic analysis. Event source unobservability, which tells as local and global adversary cannot predict the real event occurrence, even if it's manageable to collect all the information passing through the network. Event source unobservability is process of choosing dummy traffic to hide the real event sources. Add dummy traffic to the real event by add some proxies that proactively filter dummy message on their way to destination. Proxy based and tree based filtering are used in event source unobservability preserving privacy solution for sensor networks, maximally reduce the network traffic while increasing delivery ratio with sacrificing privacy level

Demerits:

- It is very difficult and expensive to achieve for resource constrained networks
- Message overhead involved in adding dummy traffic to network

F. User Centric Approach.

In real time, an individual user's location privacy needs may diverge on current time and the location. So that each user may require location privacy defense at different time and location [11]. It is desirable that the protection of location privacy is user-centric that is user can predict when to update location proof. The user centric approach, basically a distributed approach, has the vantage of not requiring a client to rely on the third party that can potentially reveal user information to adversaries. User centric approaches employ cryptographic methods in order to give the user's control over who is permitted to access location information.

Demerits:

- User centric approach imposes high costs in terms of computation and communication.
- Proof updating schedule may affect the by user centric approach.

G.VeriPlace: A Privacy-Aware Location Proof Architecture

There is a spectacular increase in the location based services this includes that of the foursquare or the yelp that contains a number of services [14]. Most of the services rely on the users for the correct location. But suppose there is a enticement user, then the users lie about that location. With the location proof architecture a users location, services proof is being collected so as to validate. Here veriPlace is being introduced with the user's privacy of high concern along with that it can detect cheating users who collect the proofs where they are not located. veriPlace integrated with yelp has proved to provide optimal privacy .

Demerits:

- Mobile Node needs to collect intermediate location proof and final location proof it may affect the computational resources.

I. L2P2.

Location privacy can be defined as information of location of events. Location privacy is thus of high concern especially for the mobile users who use the location based services provided by that of the third party with the help of the mobile networks. In recent times there has been a terrific effort on developing new anonymity to protect the location privacy of the mobile users. Even though the prior techniques assume that a user will have a stable privacy along the spatial and the temporal dimensions. In this a new problem is being defined .this is the location aware location privacy protection (L2P2)[15] where in users can diversely define diverse and dynamic privacy requirements over the different locations. The aim of the L2P2 is basically to find the smallest cloaking area for each of the location request so that the diverse requirements of the users are being satisfied over the spatial and the temporal dimension. So a set of polynomial-time heuristics is being proposed to address basic and enhanced L2P2 problems.

Demerits:

- Achieved optimal location proof accuracy**.**

J. APPLAUS.

A Privacy-Preserving Location proof Updating System (APPLAUS)[12].In APPLAUS, Mobile devices which are enables with Bluetooth mutually produce location proofs, then the location proof is insert into to a untrusted location proof server. An authorized verifier can retrieve location proofs from the server. Mobile devices use frequently updated pseudonyms to preserve and protect location privacy from each mobile device, and from an untrusted location proof server. APPLAUS is based on user-centric location privacy model in which each users evaluate their location privacy levels in real-time and make a decision whether and when to

accept a location proof request. To defend against colluding attacks, suggest betweenness ranking based and correlation clustering based approaches for outlier detection. Separation of privacy is achieved by separating the identity and location information of user.

Demerits:

- Weak identity of the device
- Bluetooth has security issues.

IV CONCLUSION

This paper compares many localization techniques (Wi-Fi access point based localization and co-located Bluetooth enabled mobile devices mutually generate location proofs) and models (simple pseudonym, multiple pseudonym, user-centric approach, k-anonymity and event source unobservability). Survey of this paper concludes APPLAUS [12] and L2P2 [15] satisfies the requirements of privacy property [11] location privacy, identity privacy and unlinkability with high computational efficiency and also reduces overhead in message, Proof delivery ratio. So it provides the location proof efficiently and preserves the location privacy with collusion resistant.

v REFERENCES

[1]. http://en.wikipedia.org/wiki/LBS
[2]. Efficient Detection of Sybil Attack based on Cryptography in VANET, International Journal of Network Security & Its Applicarions, Nov 2011
[3]. Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
[4]. A.R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Security and Privacy, 2003.
[5]. S. Saroiu and A. Wolman. Enabling new mobile applications with location proofs. In ACM HotMobile, 2009
[6]. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi. Locationbased trust for mobile user-generated content: applications, challenges and implementations. In ACM HotMobile, 2008.
[7]. M. Li, R. Poovendran, K. Sampigethaya, and L. Huang. Caravan: Providing location privacy for vanet. In Proceedings of the Embedded Security in Cars (ESCAR) Workshop
[8]. L. Butty´an, T. Holczer, and I. Vajda. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. Security and Privacy in Ad-hoc and Sensor Networks.
[9]. Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao. Towards event source unobservability with minimum network traffic in sensor networks. In ACM WiSec, 2008.
[10]. W. Luo and U. Hengartner. Proving your location without giving up your privacy. In ACM HotMobile, 2010.
[11]. Emmanouil Magkos Cryptographic Approaches forPrivacy P reservation in Location-Based Services
[12]. Z. Zhu and G. Cao. Applaus: A privacy-preserving and collusion resistance in location proof updating system IEEE INFOCOM 2011.
[13]. B. Gedik and L. Liu. A customizable k-anonymity model for p rotecting location privacy. In *IEEE ICDCS*, 2005.
[14]. Wanying luo and urs hengartner. VeriPlace: A Privacy-Aware Location Proof Architecture
[15]. Yu Wang *and* Dingbang Xu. L2P2: Location-aware Location Privacy Protection for Location-based Services