# Enabling Location Privacy And Resisting Colluding Attacks In Location Based Services For Mobile Applications

**Priyanka Prasad B. N[1] Kusuma S[2]**
[1]Student [2]Assistant Professor
[1,2] Department Of Information Science, R.N.S.I.T. College Of Engineering Bangalore, India

*Abstract*— Location Based Services (LBS) are becoming more conventional now-a-days. Apart from benefits from these LBS, there are many privacy threats.These applications cannot rely independently on the users' devices to discover and transmit location information because users have an incentive to cheat. Instead, such applications require their users to prove their locations. Unfortunately, today's mobile users lack a mechanism to prove their current or past locations. This paper presents Location Privacy - the ability to control the access of location information related to an individual. Location proofs are handed out by the wireless infrastructure (e.g., a Wi-Fi access point or a cell tower) to mobile devices. The relatively short range of the wireless radios ensures that these devices are in physical proximity to the wireless transmitter. As a result, these devices are capable of proving their current or past locations to mobile applications. In order to defend against colluding attacks, we also present betweenness ranking-based approach for outlier detection.

**Key Words:-** Colluding Attack, Location Based Services (LBS), Location Privacy, Location Proof

## I. INTRODUCTION

Nowadays, more and more location based applications and services require users to provide location proofs at a particular time and at the same time they present users significant privacy threats. An obvious one is service anonymity threat, i.e., the potential exposure of service uses. Just like regular Internet access, a user may not want to be identified as the subscriber of some LBS, especially when the service is sensitive. Therefore, an application might ask a device to prove that the device really is or was at the claimed location.

There are many kinds of location-sensitive applications. One category is location-based access control. For example, a hospital may allow patient information access only when doctors or nurses can prove that they are in a particular room of the hospital [1]. Another class of location-sensitive applications require users to provide past location proofs [4], such as auto insurance quote in which auto insurance companies offer discounts to drivers who can prove that they take safe routes during their daily commutes, police investigations in which detectives are interested in finding outif a person was at a murder scene at some time, and location-based social networking in which a user can ask for a location proof from the service requester and accepts the request only if the sender is able to present a valid location proof. The common theme across these location sensitive applications is that they offer a reward or benefit to users located in a certain geographical location at a certain time. Thus, users have the incentive to cheat on their locations.

For self-protection, it is natural and necessary for a user to withhold her true identity when requesting an LBS. However, simply using a pseudonym, or not using any identifier at all, is not sufficient. This is due to the fact that a user's location itself may be correlated with restricted spaces such as house and office to reveal her real-world identity. For example, if a location belongs to a private property, then the adversary can derive that the user is most likely the owner of the property. A single location sample may not be linked directly to a particular user, but the accumulation of a time-series sequence of her location samples will eventually reveal her identity [3]. Once the user is identified, all her visits may be disclosed.

In this paper, we propose Location privacy in a Location proof Update System which doesn't depend on expensive computing platform and extensive deployment of network infrastructure. Here Wi-Fi enabled mobile devices which are in particular range limit mutually generate location proofs and these location proofs are uploaded to location proof server which is not trustworthy. A verifier who is authorized verifies the location proofs from the server by querying the server and it also ensures privacy from every other user. Privacy is achieved by updating pseudonyms periodically for every mobile user and also from untrusted location proof server. In order to defend against colluding attacks, betweenness ranking approach for outlier detection. Thus this paper provides description about how location proof is generated and privacy is preserved and it also explains about colluding attack detection.

## II. PREFACE

Our research can be applied to the networks where mobile nodes are independent entities equipped with Wi-Fi or Bluetooth enabled devices. In this paper, we focus on Bluetooth enabled mobile devices which communicate with each other with Bluetooth protocol. Thus location proofs are Exchanged.

### *A. Generation Of Pseudonyms*

As in case of many networks, we assume a trusted online Certification Authority (CA).The role of this CA is to establish credentials for every mobile devices before it has been entered into the network. Every mobile node *i* registers with CA that preloads M set of public/private key pairs$K_i^{Pub}$,$K_i^{Prv}$. Public keys generated will be the pseudonym of node *i* and private keys will be the signature messages digitally in which validation is done with digital certificate and thus authenticity is ensured.

### *B. Threat Model*

We consider the following threats in our architecture:

1) *Dishonest Users.* A dishonest user tries to obtain location proofs that certify her presence at some place at a particular time even if she was not there. Dishonest users may achieve this goal by colluding with malicious intruders.

2) *Malicious Intruders.* A malicious intruder is not interested in obtaining location proofs for her own use but

 

offers to help other users to get location proofs on their behalf in exchange for other benefits like money.

3) *Active And Passive Eavesdroppers.* An eavesdropper records and maybe modifies communication between users, proof issuers, or applications.

We do not consider the following threats:

- Wormhole attacks. A wormhole attack takes place when a malicious party records network traffic in a region of the wireless network and replays it in another region. For example, suppose two wireless devices A and B are invisible to each other. A malicious device C within the transmission range of device A tunnels traffic from A to device B, which makes device B appear visible to A. This kind of attack is extremely hard to detect. In a location proof architecture, by launching wormhole attacks, a user may collude with several remote malicious intruders to simultaneously obtain location proofs from APs in different places. The only way to defeat wormhole attacks is to rely on dedicated hardware and distance bounding techniques since it violates design principle that there is no dedicated hardware. We don't consider this threat.
- Weak identities. Device carriers are not always the actual device owners. For example, a device may be stolen or lent to a friend by the owner. Therefore, our use of users' public keys as their identities may not be reliable, and this form of user identity is deemed a weak identity.

## III. III.LOCATION PROOF UPDATING SYSTEM

In this section, we introduce the location proof updating architecture, the protocol, and how mobile nodes schedule their location proof updating to achieve location privacy.

### *A. Architecture*

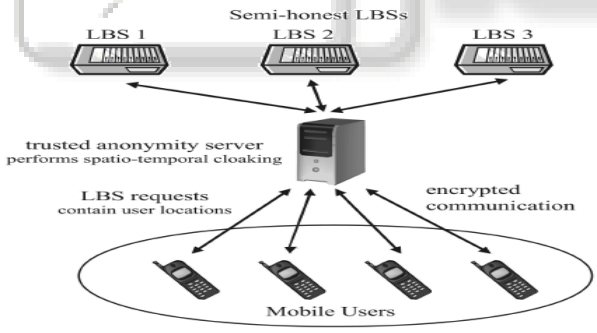


Fig. 1: Location Proof Updating Architecture and Message Flow.

We show the system architecture in Fig. 1. Mobile clients communicate with third-party LBS providers through the anonymity server. The anonymity server is a secure gateway to the semi honest LBS providers for the mobile clients. It runs a message perturbation engine, which performs location perturbation on the messages received from the mobile clients before forwarding them to the LBS provider. Each message sent to an LBS provider contains the location information of the mobile client and a time stamp, in addition to service-specific information. Upon receiving a message from a mobile client, the anonymity server removes any identifiers such as Internet Protocol (IP) addresses, perturbs the location information through spatio-temporal cloaking, and then forwards the anonymized message to the LBS provider. Spatial cloaking refers to replacing a 2D point location by a spatial range, where the original point location lies anywhere within the range. Temporal cloaking refers to replacing a time point associated with the location point with a time interval that includes the original time point.

### *B. Protocol*

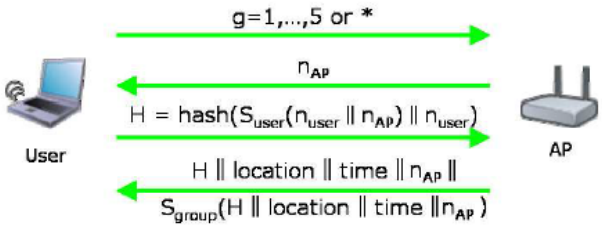


Fig. 2: Location Proof Protocol

When a user is nearby an AP, she may execute the protocol in Fig.2 to obtain location proofs from the AP. We use the user's public key as her identity, i.e. $ID_{user} = P_{user}$ where $P_{user}$ is the user's public key signed by the CA.

- The user sends a location proof request to the AP. The request should contain a desired granularity g, where g = 1… ……5 (for retroactive proofs) or g = $*$ (for proactive proofs).
- The AP generates nonce $n_{AP}$ and sends it to the user.
- The user generates nonce $n_{user}$ and sends the following hash value to the AP:

$$H = \text{hash}\,(S_{user}\ (n_{user}\ ||n_{AP})\ ||n_{user})$$

- Finally, the AP creates a location proof with a group signature and sends the proof to the user. The proof is of the following format:

$$H\ ||\ \text{location}\ ||\ \text{time}\ ||\ n_{AP}\ \ ||$$
$$S_{group}\ (H\ ||\ \text{location}\ ||\ \text{time}\ ||n_{AP})$$

The "location" part of the proof is worth further clarification.

If the user asks for a retroactive location proof by specifying a g value between one and five, the AP simply includes location information of that particular granularity. If the user requests a proactive proof, the "location" part becomes a concatenation of five cipher texts, each of which is the encrypted form of location information of a particular granularity. That is

$$\text{location} = E_{k1}(L_1)\ ||\ \cdot\cdot\cdot\ ||\ E_{k5}(L_5)$$

where $L_i$ is location information of granularity $i$, where $i$ = 1. . . 5. Moreover, the AP should also send five decryption keys ,$K_1$. . . $K_5$, to the user in this case.

## IV. SECURITY ANALYSIS AND COUNTERMEASURES

In this section, we discuss the security property in terms of source location privacy and colluding attacking, as well as the countermeasures for these threats.

### *A. Location Privacy*

There are two popular approaches to protect location privacy in the context of LBS usage: policy-based [5] and anonymity-based approaches [8]. In policy-based approaches, mobile clients specify their location privacy preferences as policies and completely trust that the third party LBS providers adhere to these policies. In the

anonymity-based approaches, the LBS providers are assumed to be semi honest instead of completely trusted. We advocate k-anonymity preserving management of location information by developing efficient and scalable system-level facilities for protecting the location privacy through ensuring location k-anonymity. We assume that anonymous location-based applications do not require user identities for providing service. For instance, a medical institution may want to release a table of medical records with the names of the individuals replaced with dummy identifiers. However, some set of attributes can still lead to identity breaches. These attributes are referred to as the *quasi-identifier*. For instance, the combination of birth date, zip code, and gender attributes in the disclosed table can uniquely determine an individual. By joining such a medical record table with some publicly available information source like a voter's list table, the medical information can be easily linked to individuals. *k-anonymity* prevents such a privacy breach by ensuring that each individual record can only be released if there are at least *k-1* distinct individuals whose associated records are indistinguishable from the former in terms of their *quasi-identifier* values.

*B. Colluding Attacks*

Another threat exists when two nodes collude with each other to generate bogus location proofs. When a malicious node $C_1$ needs to prove himself in New York City, he can have another colluding node $C_2$ to mutually generate bogus location proofs for him, with location tag of New York City. Generally, such attacks can be identified by using threshold based solution or by looking into the location traces. In threshold based solution, the system can require the prover to obtain a threshold number of witness nodes, and hence can deal with some colluding attacks. However, since it is hard for the prover to always find enough number of witness nodes, we also use the following solution. The server has information about the numbers of pseudonyms at particular time and location. This information can be used to estimate whether a prover lies about not finding enough peers or always finding the same peer based on some statistical techniques. More specifically, we are considering two-level cross validation from both location proof server and CA point of view and then integrating the results to ensure accuracy. The server-level validation is performed on individual location proof based on its timestamp and location information, where all concurrent and co-located location proofs from other pseudonyms are used to verify the reliability of the target location proof. For example, when a pair of location proofs by pseudonyms $P_A$and $P_B$are uploaded, the server checks if there are concurrent and co-located location proofs from other pseudonyms, which do not have any interaction with $P_A$and $P_B$. If there are such location proofs,$P_A$and $P_B$are suspicious to be colluders, and we then assign an appropriate trust level for the location proof.

## V. CONCLUSION

We have seen that location data can be misused in potentially damaging ways: Location privacy is important. However, location-based services are growing in popularity, and can provide significant value. The fact that location is inherently uncertain provides us an opportunity to maintain privacy while getting the benefit of location-based services.

This paper introduces location proofs, a simple mechanism that allows mobile devices to securely prove their current and past locations. We present a concrete protocol, implementable over Wi-Fi, in which APs issue location proofs to mobile devices. We then characterize the security properties of our proposed design, and we discuss the difficulties that arise from collusion attacks, such as when users share their devices with one another. In the future, we plan to build a prototype infrastructure that issues location proofs, to gain experience with applications that can use this primitive.

## REFERENCES

[1] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Security and Privacy, 2003.
[2] U.Brandes, "A Faster Algorithm for Betweenness Centrality," J. Math. Sociology, vol. 25, no. 2, pp. 163-177, 2001.
[3] S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc.Workshop Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '93), 1994.
[4] L. Buttya´n, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," Proc.Fourth European Conf. Security and Privacy in Ad-Hoc and Sensor Networks, 2007
[5] S. Capkun and J.-P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," Proc. IEEE INFOCOM, 2005.
[6] L.P. Cox, A. Dalton, and V. Marupadi, "Smokescreen: Flexible Privacy Controls for Presence-Sharing," Proc. AAACM MobiSys, 2007.
[7] E.D. Demaine, D. Emanuel, A. Fiat, and N. Immorlica, "Correlation Clustering in General Weighted Graphs," Theoretical Computer Science, vol. 361, nos. 2/3, pp. AA172-187, 2006.
[8] Z. Zhu and G. Cao, "APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-Based Services," Proc. IEEE INFOCOM, 2011.

 