ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Secrecy Preserving In a Location Proof Updating System

Babasaheb A. Waghmode, Prof. Sunita Nandgave

Student, Dept. of Computer Engineering, GHRCOEM, Savitribai Phule Pune University, Ahmednagar, MS, India

Assistant Professor, Dept. of Computer Engineering, GHRCEM, Savitribai Phule Pune University, Ahmednagar, MS, India

ABSTRACT: Today's mobile devices have inbuilt GPS systems such as smartphones which plays an important role in Location based services. In location based applications and services users require proving their current locations at a particular time. There are lots of real time applications in market that helps to track the location of the peoples. As location proof plays a critical role in enabling applications, they are location sensitive. The common gain of all the applications is that they offer geographical location of a person carrying on GPS enabled device. But sometimes users lies their present locations. The Location Based Services personalize the services they provide or grant access to resources according to the present locations of users. They are used in a variety of contexts, such as traffic monitoring, discount tied to the visit of a particular shop. In most of current schemes, the location of users or devices are determined by the device through GPS and forwarded to the Location Based Service provider. So, a user can cheat by having his or her device transmitting inexact location to gain access to unofficial or unchartered resources, thus raising the issues of verifying the position claimed by a particular user. To counter this commination, Location Based Services should ideally require the requesting device to formally prove that it really is at the claimed location. This intent has been formalized through the concept of location proof which is proving that user was at a present location at a specific moment in time. The proposed system overcomes the identity issue by using biometric server. Each users identification is stored at biometric server, biometric server lies between prover and server. The verifier usually has close relationship with the prover and biometric server to be trusted enough to gain authorization.

KEYWORDS: Location-based services, location proof, location privacy, pseudonym.

I. INTRODUCTION

Nowadays, the location based applications and services require users to provide their present location proofs at any time. For example, Google Lat-Long and Loopt are services that enable users to track friend's locations in any time. These applications are location based since location proof plays a critical role in enabling some applications. There are many kinds of location based applications. So one of them is location based access control. For e.g., a hospital may allow particular patient information access only when a nurses or doctors can prove that they are in a specific room of the hospital [5]. Another category is location based applications requires users to provide past location proofs [12], such as auto insurance quote in which insurance company offer discounts to all the drivers who can prove that they take safe routes during his daily commutes, sales officer are not in range so that time organization can track report of their rout and client so they cannot cheat with their organization, and location based social networking in which a user can ask for the exact location proof from the service requester and accepts the request only if the sender is able to give present and valid location proof. The general theme across these location sensitive applications is that they offer a rewards or benefits to users located in a secure geographical location at a certain time. Thus, users have the incentive to cheat on their actual locations. Location based sensitive applications require users to prove that they really are (or were) at the particular claimed locations. Although many mobile users have devices capable of discovering their exact locations, some users may cheat on their present locations and there is a shortage of secure mechanism to provide their current or past locations to applications and services. One feasible solution is to build a trusted computing module on each an every mobile device to make sure that the trusted GPS data is generated and transmitted. For e.g., V. Lenders proposed a solution which can be used to generate unforgettable geo tags for mobile contents such as photos and

DOI: 10.15680/ijircce.2015. 0307021

videos; however, it depends on the expensive trusted computing module on mobile devices to generate all the location proofs. Although cellular service providers have tracking services that can help to verify the present locations of gateway server in real time, so the precision is not good enough and all the location history cannot be verified correctly. Recently, several systems have been designed to let end users prove their proper locations through wireless infrastructure i.e. Wi-Fi. For e.g., S. Saroiu and A. Wolman [11] proposed a solution suitable for third party advertence, but it depends on Public Key Infrastructure and the wide deployment of Wi-Fi infrastructure. In this paper, we propose a Remote LocAtion proof Updating System and Privacy Preserving (RLAUSPP), which does not depend on the wide deployment of network infrastructure or the expen-sive trusted computing module. In RLAUSPP, gateway server devices mutually generate their exact location proofs, which are uploaded to an untrusted location proof server that can verify the trust level of each and every location proof. An authorized verifier can query and recovers all the exact location proofs from the server. Also, our location proof updating system guarantees users location privacy from every party. More explicitly, we use statistically updated pseudonyms at every mobile device to protect their location secrecy from each other, and also from the untrusted location proof server. So that we develop a user centric location based privacy model in which each and every user evaluate their current location privacy levels in real time and to choose whether and when to accept the location proof request.

A. **Problem Definition:**

Privacy is the most considered factor for the people and is the most important feature the developers to keep in mind while developing the applications. RLAUSPP stands for Re-mote LocAtion proof Updating System and Privacy Preserving. RLAUSPP architecture stands around three independents en-tities which are: the Certification Authority (CA) or Verifier, the Location proof server, the prover and witness. As location proof plays a critical role in enabling applications, they are location sensitive. Privacy and security analysis shows that the privacy property of RLAUSPP is ensured by the separation of privacy knowledge: the location proof server only knows pseudonyms and locations; the CA only knows the mapping between the real identity and its pseudonyms, while the verifier only knows the real identity and its authorized locations. Attackers are unable to learn a users location information without integrating all the knowledge. Therefore, compromising either party of the system does not reveal privacy information. The system is also resilient against collusion attacks also weak identity of device and Bluetooth has some security issues. This paper overcomes the identity issue by using biometric server. Each users identification is stored at biometric server, biometric server lies between prover and server. The verifier usually has close relationship with the prover and biometric server to be trusted enough to gain authorization.

B. **Purpose:**

Today location based sensitive services depends on users mobile devices to determine the present locations. This allows malignant users to access a limited instrument or provide dummy alibis by cheating on their present locations. Real time watch is not possible in existing system. Range of existing system is the main problem. Existing system was only works in range of Bluetooth service but proposed system works in all over the world. The best attractive application includes surveillance where urgent information is needed to decide if the people being monitored are any actual commination or an inexact goal. We have been able to create a number of different applications where we provide the user with information regarding a place he or she was. But these applications are limited to Bluetooth service only. We need to import them on gateway server services.

C. **Objective of the system:**

The main objective of project is to make existing system world wild and to bring that system to the day to day use of industrial and other business by that way we can make more easy way to connect employees with their organization and maintain the transparency between employee and owner and we can minimize the fatal occur.

D. **System Scope:**

This system is used in various scenarios of day to day market need and it is very feasible to execute in multiple type of industrial requirement.

1. Marketing company:
   In this scenario the sales executive is moving out of the company to attain their client in that case if we execute our system so the verifier form that company can easily track the location of that sales executive any they will

DOI: 10.15680/ijircce.2015. 0307021

make confirm that their sales executive are in correct location or not.

2. Hospital System:
   In multispecialty hospital lots of doctors are working by executing our system we can track that doctor location in case of emergency case.

3. Transportation Company:
4.

   In Transportation Company their drivers are moves all around the country so by executing our system we can easily track their location that they are going through correct path or if any fatal is occur so we can immediately reach to them.

II. SYSTEM ANALYSIS

A. Our Approach

This paper proposed Remote LocAtion proof Updating System and Privacy Preserving (RLAUSPP), which does not depend on the wide deployment of network infrastructure or the expensive trusted computing module. In RLAUSPP, gateway server mutually generate their location proofs, which are uploaded to untrusted location proof server that can verify the trust level of each and every users location proofs. An authorized verifier can query and recovers the exact location proofs from the server. Also, the location based proof system guarantees user location secrecy from every party. More explicitly, we use statistically updated pseudonyms at every mobile device to protect their location secrecy from each other, and also from the untrusted location proof server. This paper, mainly focus on gateway server networks where mobile devices such as cellular phones communicate with each other through gateway server. In our implementation, mobile devices periodically start location proof requests to all neighboring devices through the gateway server. After receiving a request from prover, a mobile node decides whether to exchange the location proof, based on its own location proof updating requirement and its own secrecy remuneration. Given its accurate range and low power consumption, Gateway server is a natural choice for mutual encounters and location proof exchanges.

III. IMPLEMENTATION DETAILS

In this, the system introduces the location proof updating system architecture and how mobile nodes schedule their proper location proof updating to achieve location secrecy in RLAUSPP.

1. **Prover Module:**
   In this module, the node that needs to collect present location proofs from its all the neighboring nodes. When a location proof is needed at time t1, the prover will broadcast a location proof request to its all neighboring nodes through gateway server system. If no positive response is received from the users, so that time the prover will generate a dummy location proof and submit it to the location proof server. So the prover takes the bunch of present locations from all users and sends all the proofs into encrypted form to the web server.

2. **Witness for Location:**
   Once a neighboring node agrees to provide their current location proof for the prover, this node becomes a witness node of the prover. The witness nodes will generate a present location proofs and send it back to the prover.

DOI: 10.15680/ijircce.2015. 0307021

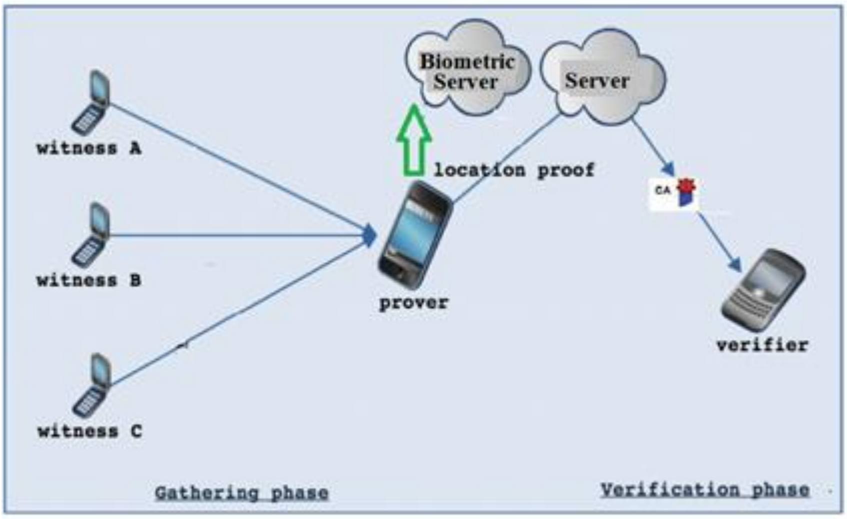

Figure 1. System Architecture

3. **Location Proof Web Server:**
   As our intent is not only to monitor the real time current locations, but also to retrieve all the current and past history location proof information when needed, a location proof web server is compulsory used to storing the history records of the location proofs. So the web server directly communicates with the prover nodes who submit their current location proofs to the prover. As the root identities of the location proofs are stored as a pseudonym, the location proof web server is untrusted in the sense that similar though it is compromised and monitored by attackers, it is difficult for the attacker to disclose the real source of the location proof. So the web server will decrypt the bunch of location proofs information of the witnesses and then forwarded to the verifier for verifying.

4. **Certificate Authority:**
   As broadly used in many networks, we consider an online Certificate Authority which is run by an independent trusted third party. Every gateway server nodes register with the Certificate Authority and preloads a set of public key and private key pairs before entering the network. Certificate Authority is the only party who knows the mapping between the actual identity and pseudonyms (i.e. public keys), and works as a bridge between the verifier and the location proof web server. It can retrieve location proof of the users from the web server and then forward this proofs to the verifier.

5. **Verifier Module:**
   A third party user or an application that is authorized to verify a provers location within a fix time period. The verifier usually has close relationship with the prover, e.g., friends, to be trusted enough to obtain authorization. The verifier verifies the bunch of location proof information of the witnesses and check the particular users are authorized or not. If the users are authorized then verifies all the users location proofs. The verifier also verifies the provers current location.

IV. ALGORITHMS

A. Clustering Algorithm

1. start

2. generate n no of parameters,

$$c = c_1 + c_2 + c_3 + ::: + c_n \qquad (1)$$

```
3. collect similar pseudonyms parameters and stored in respective classes.
4. follows each parameter within the class.

5. if same pseudonyms parameters are detected then
   create a cluster of this parameter
   else

   match rest of the cluster according to the parameter pseudonym and send it to match finding cluster.

6.  end if

    end
```

B. Encryption algorithm

```
1)    start

2)    prover collect data from witness location
3)    prover applies a private key i.e. x to collected data d and sends pair of data and key i.e. (d,k) for encryption

                    $(data,k) \rightarrow (k, data)^{e}$          (2)
4)     store the data to server
5)      if  admin is genuine then

          access the data and key (d,k) pair else
          it will restrict to access
6)      end if

7)    using key k, it will decrypt data d

                    $(k, data)^{e} \rightarrow (data)^{d}$          (3)
8)    end
```

C. Scheduling algorithm for prover

```
1)    start

2)    generate n distinct parameters

      $w_1, w_2, w_3, \ldots w_n$                          (4)
3)    generate a class for witness parameters,
      $w1 + w2 + w3 + \ldots + wn = w$ (5)
4)    for every single pseudonyms i do
5)    while current time t detect Poisson distribution
      with wi do
6)    send individual location proof to the prover
7)    if location is detected then
      submit location proof
      else
      generate and submit dummy location proof
8)    end if
9)    end while
10)   end for
```

11) end

V. RESULTS

In order to implement system work a forbidding data set is collected from World Wide Web that comprises the Latitude and Longitude of the particular location. System taking longitude and latitude from by this we will find a location of that witness.

Fig.2 shows that Proposed System RLAUSPP has better average delay than APPLAUS which is existing system. Fig. 3 shows the performance comparisons between proposed scheme and the existing scheme under different ratio of Tproof=Tcontact, where Tproof is the required interval between two location proof updates, and Tcontact is the mean real node contact interval. The proof delivery ratio of proposed system significantly outperforms over RLAUSPP and the existing scheme.

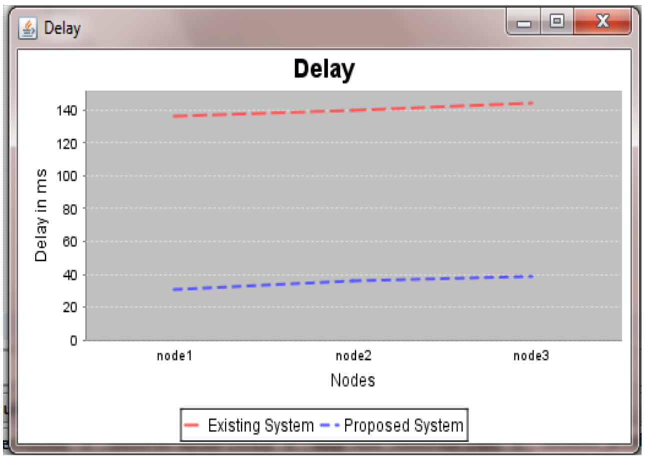

Figure 2. Average Delay

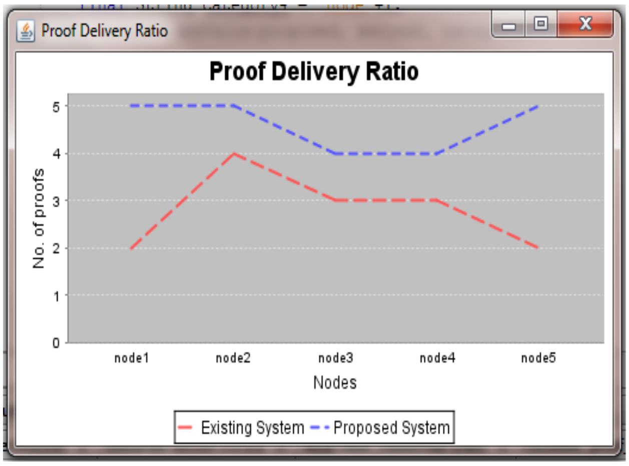

Figure 3. Proof Delivery Ratio

VI. EXPERIMENTAL SETUP

To evaluate RELAUSPP scheme performance on the techniques presented in the previous sections. The prototype has two software components: client and server. The client is implemented in JAVA (J2ME) and use CLDC emulator to show mobile users and GPS System. It can communicate with the server anytime data service. The server is implemented on a 1.90 GHz 8 GB RAM laptop. It stores the uploaded user's location proof records and manages corresponding indices using MySQL 5.0. Use J2ME Emulators to communicate with each other to test our solution.

VII. RELATED WORK

In general approach, Location based sensitive applications require users to prove that they really are (or were) at the particular claimed locations. Although many mobile users have devices capable of discovering their exact locations, some users may cheat on their present locations and there is a shortage of secure mechanism to provide their current or past locations to applications and services. One feasible solution is to build a trusted computing module on each and every mobile device to make sure that the trusted GPS data is generated and transmitted. For e.g., V. Lenders proposed a solution which can be used to generate unforgettable geo tags for mobile contents such as photos and videos; however, it depends on the expensive trusted computing module on mobile devices to generate all the location proofs. Although cellular service providers have tracking services that can help to verify the present locations of gateway server in real time, so the precision is not good enough and all the location history cannot be verified correctly. Recently, several systems have been designed to let end users prove their proper locations through wireless infrastructure i.e. Wi-Fi. For e.g., S. Saroiu and A. Wolman [11] proposed a solution suitable for third party advertence, but it depends on Public Key Infrastructure and the wide deployment of Wi-Fi infrastructure. Recently, discrete systems have been proposed to provide end users the ability to prove that they were moving in a particular place at a particular time. The solution in depends on the fact that nothing is faster than the speed of light in order to enumerate an over limit of a particular users distance. S. Capkun and J.P. Hubaux propose challenge response schemes, which use multiple receivers to correctly estimate a wireless node proper location using RF propagation characteristics. In the authors describe a certain localization service that can be used to produce unforgettable geo tags for mobile things or contents such as photos and video. However dedicated size hardware or high expenses trusted computing module is required. S. Saroiu and A. Wolman [11] propose a solution suitable for third party advertency, but it depends on a Public Key Infrastructure and the vast deployment of wireless infrastructure (i.e. Wi-Fi). Separate from these solutions, RLAUSPP uses a peer to peer and client server approaches and doesnt require any changes to the existing infrastructures. Cox, Dalton, and Marupadi introduces a presence sharing mobile social duty between collocated users which depends on centralized, trusted brokers to coordinate innominate communication between strangers.

However, this service doesnt reveal the proper location information to the service provider thus can only provide exact location proofs between two users who have actually encountered. RLAUSPP can provide correct location proofs to third party by uploading actual encounter location to the untrusted server while maintaining location secrecy. There are lots of existing works on location secrecy in wireless networks. In the authors M. Gruteser and D. Grunwald are proposed to reduce or mitigate the precision of location information along spatial and/or temporal dimensions. Separate from them, our approach doesnt require the actual location proof web server to be trustworthy. Xu and Cai [10] propose a feeling based model which allows a users to express their secrecy requirement. One important concern here is that the spatial and temporal correlation between successive locations of mobile nodes must be carefully eliminated to prevent external parties from compromising their proper location secrecy. The techniques in [9] achieve location secrecy by changing pseudonyms in regions called mix zones. In our system, pseudonyms of every node are changed by the node itself time to time following a Poisson distribution, rather than being exchanged between two untrusted nodes. Identifying a fundamental tradeoff between performance and privacy, Shao et al. propose a notion of statistically strong source anonymity in wireless sensor networks for the first time, while Li and Ren [6] and Zhang et al. tried to provide source location privacy against traffic analysis attacks through dynamic routing or anonymous authentication. Our plan uses equal root location unobservability concept in which the correct location based proof message is scheduled through statistical algorithms. However, their focus is to generate identical distributions between different nodes to hide the actual event source, while our focus is to design different distributions between the distinct pseudonyms to protect the actual identity of the user.

VIII. CONCLUSION AND FUTURE SCOPE

The proposed system uses a Remote location proof updating system and privacy preserving called Secure RLAUSPP, where GPS locations are used to generate location proofs and upload to server. By using Biometric server to identify devices more accurately and for security, in the proposed system the pseudonyms are generated randomly which helps to protect each device source location from other devices. Also develop a user centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept a location proof exchange request based on their location privacy levels.

Build system in Android. As well as ios, windows, bada etc. Provide free service Google provides simulated environment and standard development kit for developing Android applications. Although this platform is very new and SDK provided is still in its nascent stage, a great number of mobile companies are queuing up to install it on their devices. We chose Android as it is parallel to iOS (supported by Apple) in terms of facilities it provide and is also open source.

ACKNOWLEDGMENT

I express great many thanks to Prof. Sunita Nandgave for her great effort of supervising and leading me, to accomplish this fine work. Also to college and department staff, they were a great source of support and encouragement. To my friends and family, for their warm, kind encourages and loves. To every person gave us something too light my pathway, I thanks for believing in me.

REFERENCES

1. Z. Zhu and G. Cao, Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System, IEEE MOBILE COMPUTING, VOL. 12, NO. 1, 2013.
2. M. Talasila, R. Curtmola, and C. Borcea. Link: Location verification through immediate neighbors knowledge.In P. S enac, M. Ott, and A. Seneviratne, editors, Mobile and Ubiquitous Systems: Computing, Networking,and Servi ces, volume 73 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pages 210 223. Springer Berlin Heidelberg, 2012
3. Z. Zhu and G. Cao. Towards privacy-preserving and colluding-resistance in location proof pdating system. IEEE Transactions on Mobile Computing , 99(PrePrints), 2011
4. M. Fiore, C. Casetti, C.-F. Chiasserini, and P. Papadimitratos. Discovery and verification of neighbor positions in mobile ad hoc networks.IEEE Transactions on Mobile Computing , 99 2011.
5. W. Luo and U. Hengartner, Proving Your Location Without Giving Up Your Privacy, Proc. ACM 11th Workshop Mobile Computing Systems and Applications (HotMobile 10), 2010.
6. Y. Li and J. Ren, Source-Location Privacy Through Dynamic Routing in Wireless Sensor Networks, Proc. IEEE INFOCOM, 2010.
7. J. Manweiler, R. Scudellari, and L.P. Cox, SMILE: Encounter- Based Trust for Mobile Social Services, Proc. ACM Conf. Computer and Comm. Security (CCS), 2009.
8. J. Manweiler, R. Scudellari, Z. Cancio, and L.P. Cox, We Saw Each Other on the Subway: Secure Anonymous Proximity-Based Missed Connections, Proc. ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile 09), 2009.
9. J. Freudiger, M.H. Manshaei, J.P. Hubaux, and D.C. Parkes, On Non- Cooperative Location Privacy: A Game-Theoretic Analysis, Proc. 16th ACM Conf. Computer and Comm. Security (CCS), 2009.
10. T. Xu and Y. Cai, Feeling-Based Location Privacy Protection for Location-Based Services, Proc. 16th ACM Conf. Computer Comm. Security (CCS), 2009.
11. S. Saroiu and A. Wolman, Enabling New Mobile Applications with Location Proofs, Proc. ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile 09), 2009.
12. Muthu,Vinothkumar, Einstein, Subala AASLTU: An Advanced System for Location Tracking and Updating\