International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

A SECURE AND LOCATION PROOF SYSTEMS FOR REQUIREMENTS, TAXONOMY, AND COMPARATIVE ANALYSIS

K.VASANTHA[1], D.ANAND [2]
[1] PG SCHOLAR, DEPT OF CSE, ST.MARY'S GROUP OF INSTITUTION, GUNTUR, AP, INDIA.
[2]ASST. PROFESSOR[M.TECH], DEPARTMENT OF CSE, ST.MARY'S GROUP OF INSTITUTION, GUNTUR, AP, INDIA.

ABSTRACT: Recently, there has been a rapid growth in location based systems and applications in which users submit their location information to service providers in order to gain access to a service, resource, or reward. We have seen that in these applications, dishonest users have an incentive to cheat on their location. Unfortunately, no effective protection mechanism has been adopted by service providers against these fake location submissions. This is a critical issue that causes severe consequences for these applications. Motivated by this, we propose the Privacy-Aware and Secure Proof Of proximity (PASPORT) scheme in this article to address the problem. Using PASPORT, users submit a location proof (LP) to service providers to prove that their submitted location is true. PASPORT has a decentralized architecture designed for *ad hoc* scenarios in which mobile users can act as witnesses and generate LPs for each other. It provides user privacy protection as well as security properties, such as enforceability and non transferability of LPs. Furthermore, the PASPORT scheme is resilient to prover–prover collusions and significantly reduces the success probability of Prover–Witness collusion attacks. To further make the proximity checking process private, we propose P-TREAD, a privacy-aware distance bounding protocol and integrate it into PASPORT. To validate our model, we implement a prototype of the proposed scheme on the Android platform. Extensive experiments indicate that the proposed method can efficiently protect location-based applications against fake submissions.

1.INTRODUCTION

THE recent advances in the smart phone technology and positioning systems has resulted in the emergency of a variety of location-based applications and services [1]–[3], [48], such as activity-tracking applications, location-based services (LBSs), database-driven cognitive radio networks (CRNs), and location-based access control systems. In these applications, mobile users submit their position data to a location-based service provider (LBSP) to gain access to a service, resource, or reward. These applications are very popular due to the useful services they offer. According to recent business reports, the market value of LBSs was U.S. $20.53 billion in 2017 and is anticipated to reach U.S. $133 billion in 2023, with an expected annual growth rate of 36.55% [4].

However, LBSPs are vulnerable to location spoofing attacks since dishonest users are incentivized to lie about their location and submit fake position data [5]–[9]. Now, we present some examples to highlight the relevant issues in these applications. In the current online rating and review applications, users' real location is not verified, which enables them to submit fake positive or negative reviews for their own business or their rivals [10], [11].

Furthermore, in CRNs [6], [8], [16], malicious users can submit fake locations to the database to access channels that are not Available in their location. In location-based access control applications [18]–[20], attackers can gain unauthorized access to a system or resource by submitting fake location claims. In activity-tracking applications, insurance companies may offer health insurance plans in which customers are offered discounts if they have a minimum level of physical activity [7], [12]–[15]. This creates an incentive for dishonest user to cheat on their location data. Thus far, with these examples, it is clear that preventing fake location submissions in these applications is still an open challenge. To protect these applications against location spoofing attacks, a number of location proof (LP) schemes have been proposed. Using these mechanisms, a mobile device (called a prover in the literature) receives one or more LPs from its neighbor devices when it visits a site.

The prover then submits the received LPs to the LBSP as a location claim. The LBSP checks the submitted LPs and either accepts or rejects the user's claim. LP schemes is categorized into two groups depending on the system architecture: centralized or distributed. In the centralized mechanisms [21]–[24], a trusted wireless infrastructure [such as a WiFi access point (AP)] is employed to generate LPs for mobile users. In distributed schemes [25]–[30], mobile users act as witnesses and generate LPs for each other. The latter approach is useful for scenarios in which there is no wireless infrastructure at the desired locations or it is expensive to employ a large number of APs for different locations. In our extensive literature review and to the best of our knowledge, we observed that all the current LP schemes suffer from at least one key drawback.

First, some of these schemes are vulnerable to prover–prover (P–P) collusions [22], [25], [2]. In this attack, a remote malicious prover colludes with a dishonest user (located at a desired site) to obtain an LP. The dishonest user submits an LP request to the neighbor witness devices on behalf of the remote prover. This security threat is called terrorist fraud in the literature [31], [32] (see Section III-A for more details). Second, none of the current distributed schemes offer a reliable solution for Prover–Witness (P–W) collusions. In this attack, a dishonest user acts as a witness for a remote malicious prover and generates a fake LP for him [25]. Note that this security threat is specific to the distributed LP schemes only since witnesses are not trusted in this type of scheme. Finally, in some schemes, location privacy has not been considered [21], [23], [28], i.e., users broadcast their identity for neighbor devices or a third party server during the LP generation or submission process. In addition, there are other challenges with the current schemes, such as high level of communication and computation overheads [26] and expensive implementation [21], [24].

2.LITERATUREREVIEW

Security and privacy in location-based services for vehicular and mobile communications by P. Asuquo et al

Location-based services (LBSs) have gained popularity as a result of the advances in mobile and communication technologies. LBS provide users with relevant information based on their location. In spite of the desirable features provided by LBS, the geographic locations of users are not adequately protected. Location privacy is one of the major challenges in vehicular and mobile networks. In this paper, we analyze the security and privacy requirements for LBS in vehicular and mobile networks. Specifically, this paper covers privacy enhancing technologies and cryptographic approaches that provide location privacy in vehicular and mobile networks. The different approaches proposed in literature are compared and open research areas are identified.

A survey of fingerprint-based outdoor localization by Q. D. Vo and P. De

A growing number of sensors on smart mobile devices has led to rapid development of various mobile applications using location-based or context-aware services. Typically, outdoor localization techniques have relied on GPS or on cellular infrastructure support. While GPS gives high positioning accuracy, it can quickly deplete the battery on the device. On the other hand, base station based localization has low accuracy. In search of alternative techniques for outdoor localization, several approaches have explored the use of data gathered from other available sensors, like accelerometer, microphone, compass, and even daily patterns of usage, to identify unique signatures that can locate a device. Signatures, or fingerprints of an area, are hidden cues existing around a user's environment. However, under different operating scenarios, fingerprint-based localization techniques have variable performance in terms of accuracy, latency of detection, battery usage. The main contribution of this survey is to present a classification of existing fingerprint-based localization approaches which intelligently sense and match different clues from the environment for location identification. We describe how each fingerprinting technique works, followed by a review of the merits and demerits of the systems built based on these techniques. We conclude by identifying several improvements and application domain for fingerprinting based localization.

An exploration to location–based service and its privacy preserving techniques: A survey by R. Gupta and U. P. Rao

Mobile gadgets today are swaggering computing potential and memory at par or at times even higher to that found in desktop personal computers. A wireless interconnection has turned out to be considerably more readily accessible these days. As individuals are growing mobile with regard to the fast lifestyle and working pattern, a new, smarter system came into existence that is termed as 'Location Based Service' (LBS). Such a system amalgamates the location data of a user with smart applications to deliver demanded services. Although LBS provide major openings for a large variety of markets and remarkable convenience to the end user, it also presents subtle privacy attack to user's location information. Threat to the privacy sneaks into the system due to the prerequisite of sending user's current location to the LBS provider to attain related services. Since the volume of data gathered from dynamic or stationary mobile users using LBS can be high, it is vital to outline the frameworks and systems in a manner that is secure and keep the location information private. In this paper, we perform an exploratory survey about the various techniques that have been suggested by many researchers based on centralized and distributed approaches, to preserve location privacy of the user. A large portion of these techniques has a trade-off between privacy, efficiency, applicability and quality of service. This paper details and analyses the various existing techniques for preserving location privacy of the participating user in LBS.

3.EXISTING SYSTEM

To address this issue, Saroiu and Wolman [23] proposed a technique in which the AP broadcasts beacon frames consisted of a sequence number. To obtain an LP, users must sign the last transmitted sequence number with their private key and send it back to the AP along with their public key (the access point broadcasts beacons every 100 ms). This makes the system resistant against terrorist frauds since the malicious prover does not have enough time to receive the sequence number from the adversary and sign and send it back to the adversary. However, the proposed algorithm has privacy issues because users must reveal their identity publicly. Javali *et al.* [21] have used the same idea to make their algorithm resistant against relay attacks. They also utilize the unique wireless channel characteristics, i.e., channel state information (CSI) to decide on users' proximity. The proposed scheme consists of three entities, i.e., AP, verifier, and server, which make the system expensive. In addition, the user's identity is revealed publicly, which might cause privacy issues.

Davis *et al.* [27] proposed a privacy-preserving alibi (LP) scheme that has a distributed architecture. To preserve users' location privacy, in the introduced scheme, their identity is not revealed, while an alibi is being created. Thus, only a judge with whom a user submits his/her alibi can see the user's identity. However, collusions and other security threats have not been considered in this article.

In the distributed solutions, Prover-Witness collusions are possible because witness devices are not always trusted. A witness device can issue an LP for a dishonest user, while one of them (or both) is not located at the claimed location. This is one of the major challenges of these schemes. For example, in PROPS that has been proposed by Gambs *et al.* [30], Prover-Witness collusions have not been discussed although it provides an efficient and privacy-aware platform for users to create LPs for other users.

STAMP introduced by Wang *et al.* [25] is another example in which an entropy-based trust model is proposed to address the Prover-Witness collusions issue. This method is also unable to provide the necessary reliability to detect Prover-Witness collusions. In addition, to address terrorist frauds, STAMP employs the Bussard-Bagga protocol [31] as the DB protocol that has already been shown to be unsafe [34]-[36]. Moreover, the computation time required by STAMP to create an LP is long when users have a large private key [25]. Although different novel methods have been introduced so far, each of them has its own constraints, i.e., privacy issues [21], [23], [28], vulnerability against collusions [22], [25]–[28], [30], high level of communication and computation overheads [26], and expensive for implementation [21], [24]. The scheme proposed in [29] prevents P–W collusions only in crowded scenarios.

In the existing work, the system is not providing Resistance to Sybil Attacks.

There is no Resistance to Witnesses Collusions techniques.

4. PROPOSED SYSTEM

The proposed system architecture is shown in Fig. 3. As we see, the system has a distributed architecture and consists of three types of entities, i.e., prover, witness, and verifier. A prover is a mobile user who requires to prove his/her location to a verifier. A witness is the entity that accepts to issue an LP for a neighboring prover upon request. We assume that service providers create sufficient incentives for mobile users to become a witness and certify other users' location. In PASPORT, we consider witnesses as mobile users.

Finally, a verifier is the unit that is authorized by the service provider to verify LPs claimed by provers. We assume that provers communicate with witnesses through a short-range communication interface, such as Wi-Fi or Bluetooth. This short range communication channel is supposed to be anonymous such that users can broadcast their messages over it without revealing their identifying data, such as IP or MAC address.

The system is more effective due to LBSPs can incentivize mobile users to collaborate by offering them some rewards, badges, and benefits that they are currently providing to their users.

The system is more effective due to another approach is to integrate an incentive mechanism into the proposed scheme, e.g., using a block chain architecture that remunerate users with a given amount of a crypto currency.

5. SYSTEM ARCHITECTURE:

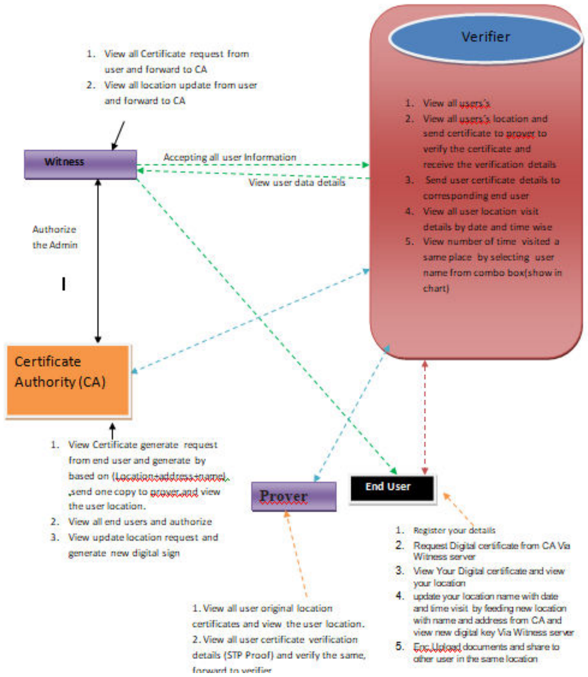

1. View all Certificate request from user and forward to CA
2. View all location update from user and forward to CA
Witness
Accepting all user Information
View user data details
Authorize the Admin
I
Certificate Authority (CA)
1. View Certificate generate request from end user and generate by based on (Location+address+name), ,send one copy to prover and view the user location.
2. View all end users and authorize
3. View update location request and generate new digital sign
Verifier
1. View all users's
2. View all users's location and send certificate to prover to verify the certificate and receive the verification details
3. Send user certificate details to corresponding end user
4. View all user location visit details by date and time wise
5. View number of time visited a same place by selecting user name from combo box(show in chart)
Prover
End User
1. View all user original location certificates and view the user location.
2. View all user certificate verification details (STP Proof) and verify the same, forward to verifier
1. Register your details
2. Request Digital certificate from CA Via Witness server
3. View Your Digital certificate and view your location
4. update your location name with date and time visit by feeding new location with name and address from CA and view new digital key Via Witness server
5. Enc Upload documents and share to other user in the same location

Fig 1 architecture Diagram

6.IMPLEMENTATION

WITNESS SERVER

In this module, the Witness Server has to login by using valid user name and password. After login successful he can perform some operations such as viewing all Certificate Requests from Users and Forwarding to CA and Viewing all Location Update from users and Forwarding to CA.

Viewing all Certificate Request from User and Forward to CA

In this module, the witness server views all Certificate Request details (username, sent from location and address, and the date) sent by Users and Forwards those requests to Certificate Authority.

CERTIFICATE AUTHORITY(CA)

In this module, the Certificate Authority has to login by using valid user name and password. After login successful he can perform some operations such as viewing all

Certificate Requests from Users and Generating , Viewing and Authorizing all End Users, Viewing Update Location Requests from Users and Generate new Digital Sign.

View Certificate Generate Request and Generate

In this module, the Certificate Authority views all user request for certificates and CA generates Certificate based on Location+Address+Name of Corresponding user and sends one copy of Generated Certificate to Prover Authority.

View all End Users and Authorize

In this module, the CA views all user details (Username, Email-ID, Mobile Number, Location and Image of User) and authorizes them as permission for their login.

View all Update Location Requests and Generate Certificate (new Digital Sign)

In this module, the CA views all user update location requests and generates Digital Sign (Certificate) based on their new Location+new Address+Name and Sends one copy of generated certificate to prover authority.

PROVER AUTHORITY

In this module, the Prover Authority has to login by using valid user name and password. After login successful he can perform some operations such as viewing all user Original Location Certificates and Viewing their Location and Viewing all user Certificate Verification Details and Verifying it and Forwarding back to Verifier.

View all User Original Location Certificates and Their Location

In this module, the Prover Authority views all user Original (Updated or Current) Location Certificates and View the User Location.

View all User Certificate Verification Details and Verify

In this, the Prover view and verifies all user Certificate Verification details (username, Digital Certificate, User Location, Request Date and Status of it) sent by Verifier for Verification. If the Status is Pending then the prover verifies certificate details with the copy present with him/her (prover) sent by CA while generating. If the details matches then it will send back to Verifier by updating status as Verified or if certificate does not matches then the status will updated as Certificate Mismatch and Forwards back to Verifier.

VERIFIER AUTHORITY

In this module, the Verifier Authority has to login by using valid user name and password. After login successful he can perform some operations such as viewing all user’s location, Viewing all user’s location and send certificate to prover for verification, sending user certificate details to corresponding users, viewing all user location visit details by date and time wise and viewing number of times visited a same place by selecting user name.

View all User’s location and send Certificate to Prover for Verification

In this, the verifier views all user location and send user’s certificate details(username, location and certificate) to prover to verify the details and gets the verification results from the prover.

Send user Certificate Details to Users

In this, the verifier views and send certificate details (Certificate includes Digital Sign Generated based on user’s Location+Address+Username) to corresponding users.

View all user location visit details by date and time wise

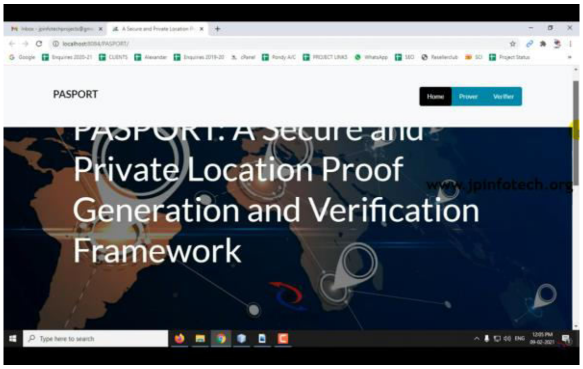
In this, the verifier views all user location visit details by date and time wise. The Visit details means the user's all updated location details and the date and time.

View number of times the user visited a same place in chart

In this, the verifier can view number of times the user visited the place by updating his location. By selecting the users, the verifier can see the visit counts.

.

7.SCREEN SHOTS



PASPORT: A Secure and Private Location Proof Generation and Verification Framework

8.CONCLUSION

This article proposed a secure and privacy-aware scheme for LP generation and verification. The proposed scheme has a decentralized architecture suitable for ad hoc applications in which mobile users generate LPs for each other. To address terrorist frauds, we developed a DB protocol P-TREAD, that is, a private version of TREAD, and integrated it into PASPORT. Using P-TREAD, a dishonest prover who established a prover-prover collusion with an adversary can easily be impersonated by the adversary later. Thus, no logical user takes such a risk by initiating a prover–prover collusion. Furthermore, we employed a witness selection mechanism to address the prover–witness collusions. Using the proposed mechanism, available witnesses are randomly assigned to requesting provers by the verifier. This prevents malicious provers from choosing the witnesses themselves.

The main strengths of the proposed scheme are: 1) no central trusted entity is required to operate as a witness device; 2) it has reliable performance against prover–prover and prover– witness collusions to which majority of the current schemes are vulnerable; 3) our prototype implementation shows that the LP generation process in the proposed scheme is faster than the existing schemes; and 4) it preserves users' location privacy as P-TREAD DB protocol enables users to anonymously broadcast their messages for the neighbor witnesses during the LP generation process.

As a future work direction, we intend to extend the PASPORT scheme such that it provides location granularity feature. Using these users can select to which level their location data is revealed. Moreover, designing a block chain based incentive mechanism to encourage users to collaborate with the system can be another research direction for this article.

BIBILOGRAPHY

[1] P. Asuquo et al., "Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures," IEEE Internet Things J., vol. 5, no. 6, pp. 4778–4802, Dec. 2018.

[2] Q. D. Vo and P. De, "A survey of fingerprint-based outdoor localization," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 491–506, 1st Quart., 2016.

[3] R. Gupta and U. P. Rao, "An exploration to location–based service and its privacy preserving techniques: A survey," Wireless Pers. Commun., vol. 96, no. 2, pp. 1973–2007, 2017.

[4] Global Location–Based Services Market (2018–2023). Accessed: Jul. 20, 2019. [Online]. Available: https://www.businesswire.com/news/ home/20180927005490/en/Global–Location-based-Services-Market-2018-2023-Projected-Grow

[5] Y. Zheng, M. Li, W. Lou, and Y. T. Hou, "Location based handshake and private proximity test with location tags," IEEE Trans. Depend. Sec. Comput., vol. 14, no. 4, pp. 406–419, Jul./Aug. 2017.

[6] Y. Li, L. Zhou, H. Zhu, and L. Sun, "Privacy–preserving location proof for securing large–scale database–driven cognitive radio networks," IEEE Internet Things J., vol. 3, no. 4, pp. 563–571, Aug. 2016.

[7] A. Pham, K. Huguenin, I. Bilogrevic, I. Dacosta, and J. P. Hubaux, "SecureRun: Cheat–proof and private summaries for location–based activities," IEEE Trans. Mobile Comput., vol. 15, no. 8, pp. 2109–2123, Aug. 2016.

[8] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2751–2759.

[9] Z. Zhang et al., "On the validity of geosocial mobility traces," in Proc. ACM Workshop Hot Topics Netw. (HotNets), 2013.

[10] D. Bucher, D. Rudi, and R. Buffat, "Captcha your location proof—A novel method for passive location proofs in adversarial environments,"in Proc. 14th Int. Conf. Location Based Services, 2018, pp. 269–291.

[11] A. Mukherjee, B. Liu, and N. Glance, "Spotting fake reviewer groups in consumer reviews," in Proc. 21st Int. Conf. World Wide Web (WWW), 2012, pp. 191–200.

[12] Nike+ Badges and Trophies. Accessed: Jul. 20, 2019. [Online]. Available: http://www.garcard.com/nikeplus.php

[13] Higi. Higi: Know Your Numbers. Own Your Health. Accessed: Jul. 20, 2019. [Online]. Available: https://higi.com

[14] Oscar Health Using Misfit Wearables To Reward Fit Customers. Accessed: Jul. 20, 2019. [Online]. Available: http://www.forbes.com/sites/stevenbertoni/2014/12/08/oscarhealth-using-misfit-wearables-toreward-fit-customers

[15] Health Insurer's App Helps Users Track Themselves. Accessed: Jul. 20, 2019. [Online]. Available: http://www.technologyreview.com/ news/516176/healthinsurers-app-helps-users-track-themselves

[16] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Location privacy preservation in database–driven wireless cognitive networks through encrypted probabilistic data structures," IEEE Trans. Cogn. Commun. Netw., vol. 3, no. 2, pp. 255–266, Jun. 2017.

[17] K. Zeng, S. K. Ramesh, and Y. Yang, "Location spoofing attack and its countermeasures in database-driven cognitive radio networks," in Proc. IEEE Commun. Netw. Secur. (CNS), Oct. 2014, pp. 202–210.

[18] A. van Cleeff, W. Pieters, and R. Wieringa, "Benefits of location-based access control: A literature study," in Proc. IEEE/ACM Int. Conf. Green Comput. Commun., Dec. 2010, pp. 739–746.

[19] Y. Baseri, A. Hafid, and S. Cherkaoui, "K-anonymous location-based fine-grained access control for mobile cloud," in Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2016, pp. 720–725.

[20] E. Androulaki, C. Soriente, L. Malisa, and S. Capkun, "Enforcing location and

time–based access control on cloud–stored data," in Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2014, pp. 637–648.