DOI:10.21276/sjeat

Saudi Journal of Engineering and Technology
Scholars Middle East Publishers
Dubai, United Arab Emirates
Website: http://scholarsmepub.com/

ISSN 2415-6272 (Print)
ISSN 2415-6264 (Online)

Original Research Article

Secure Location Tracker for Mobile Devices by providing Witness

Pooja Bhat[1], Dr. S Meenakshi Sundaram[2], Pooja Deshpande[1], Pooja T U [1], Shwetha G Navadagi [1]
[1]Student, GSSS Institute of Engineering and Technology for Women, Mysuru, India
[2]Professor and Head, Department of CSE, GSSS Institute of Engineering and Technology for Women, Mysuru, India

***Corresponding Author:**
Pooja Bhat
Email: poojabhatpb1995@gmail.com

Abstract: In recent years, location of mobile devices has become an important factor. 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 devices. Location based services allow users to access services based on the users geographical information. The service is mainly based on location proof which is given by the user and the presence of the user at the given location at a given time. We propose a witness oriented asserted location provenance framework by providing a witness and we also generate the cryptoID for each user. This is based on asserted location proof protocol (ALP). We preserve the location information of the user for a long time. Witness oriented application features a web-based service provider, a desktop-based location authority server, an Android-based user app, and a desktop-based auditor. The results show location proofs effectively, which significantly preserve the source location.
Keywords: User, Witness, Location Authority, Asserted location, Provenance, Location Proof.

INTRODUCTION

Mobile devices uses location based service by using users geographical location. Location based services concentrates on location proof. The location proof is provided by the users. Later the auditor verifies whether the given proof is correct or not with respect to user identity, location of the user and also when the user is present in that location along with time and date. The false location reporting implications have the unimportant matters. This is a Witness ORiented Asserted Location provenance framework (WORAL) [1]. The system is based on the Asserted Location Proof (ALP) protocol and we refer the OTIT model [3]. Using this model we provide the secure location provenance. We use Witness ORiented application in web-based service provider, a desktop-based location authority server, an Android-based user app, and a desktop-based auditor.

The objectives of the proposed work are as follows:
1) To provide a witness that is responsible to ensure whether the user is present in current location at the given time.
2) To generate a cryptoID, which is unique to the user. By using this key we can uniquely differentiate each user.
3) To store the user data for long time.
4) To have the Witness ORiented framework that supports Android based devices to collect and export location proofs.
5) To develop a secure protocol for Witness ORiented based on location proofs and augmented the protocol using secure location provenance preservation.

Assertion oriented location provenance schemes can be effectively used in a variety of real-life scenarios. Our solution emphasizes the device's presence, and can be a highly applicable technology for equipment handling businesses. At present, most high end devices come with networking features and built-in memory. Hence, these expensive devices could easily be monitored for presence at their particular locations. The concept of location provenance and witnesses can also be applied to other domains, such as in preserving the integrity of supply chain information for different products and services.

The following analogy illustrates the practicality of a secure and asserted location provenance framework. Bob is an engineer at a construction company. The company requires Bob to travel to the construction sites and create a daily report of the project status. Unfortunately, Bob is charged with negligence towards his job when the company suffered a major loss due to an accident. The inspection report

that Bob presented was discarded for being a false document as the company claimed that Bob did not visit the construction site and the accident was a result of his negligence. In an alternate scenario, Bob collects location provenance records as he visits each of the construction sites, which are asserted by the site engineer as a witness. Therefore, Bob can then prove his regular visits and the order of visit to each of the sites based on the secure location provenance records. Our work presents the Witness ORiented Asserted Location provenance framework. The system is based on the Asserted Location Proof (ALP) protocol and incorporates the OTIT model for secure location provenance. The Witness ORiented framework is a complete suite of production-ready applications, featuring a web-based service provider, a desktop-based location authority server, an Android-based user app, and a desktop-based auditor. Our proposed work helps in providing long term authentication and accountability of location tracking history information or path of an entity [9].

RELATED WORK

Ragib Hasan, [1] *et al*. presented a work on location-based access control (LBAC), where, the requester, the access control engine, and the location service allows evaluation of LBAC policies for accessing resources and services, according to the location of the user with respect to a particular area. Rasib Khan [2] *et al.* proposed ALARM; a location aided routing protocol, which uses current location of nodes to construct the network topology and forward data in mobile ad-hoc networks. In another similar work, proposed PRISM, a secure and privacy preserving on-demand reactive location-based anonymous routing protocol for mobile ad-hoc networks. Traditional Global Positioning Systems (GPS) are not suitable in terms of security and indoor tracking. Gonz Alez Tablas [9] utilized multi-channel information from Caller-ID, GPS, cellular telephony, and satellite ranging, in a combined approach to determine the movement and location of user devices. Unfortunately, malicious entities can bypass such combinatorial schemes. GPS signatures are not useful since they are open to spoofing attacks [11]. J Brassil *et al* [6]. have shown how localization algorithms are vulnerable to non-cryptographic attacks using a low-cost directional antenna. The proposed schemes also do not consider preserving the order in which the location proofs were obtained by the user. Bharathi *et.al* [8] proposed that APPLAUSE can be implemented with the existing network infrastructure and the current mobile devices, with some power cause and computation. It can be easily deployed in wireless or mobile devices. M. Winslett *et.al*[13] proposed the Case of the Fake Picasso where they presented the empirical results that show that, for typical real-life workloads, the runtime overhead of our approach to recording provenance with confidentiality and integrity guarantees ranges from 1% – 13%.

A **Service Provider** SP is a trusted entity who provides the secure location provenance services to mobile users. It is not a centralized model. Service Providers include certified location authorities and verified auditors. A **User** U is an entity who visits a particular location and uses a mobile device to request the cryptoID and store location provenance records. A **Location Authority** LA is stationary, who is been certified by the SP, identified using a unique identifier, and is responsible for providing location provenance records for a particular area. A **Witness** W is a mobile user who has volunteered to assert a location provenance record for the presence of another mobile device user at the given location. A **Witness List** WL provides the list of all registered witnesses under the coverage of the location authority at a given time. A **CryptoID** CID is a cryptographic identity for the user (who is also a witness), used in all phases of the protocol, ensuring privacy of the entities participating in the process. A **Location Proof** LP is an evidence received by a user when visiting a specific site. It compares many localization techniques and models [16]. Asserted Proof AP is a location proof LP asserted by a valid witness using his Crypto-ID. An **Auditor** is a SP verified authority who is presented with a chain of asserted location proofs and confirms the user's claim of presence at the particular site and the order of visits.

PROPOSED WORK

Here we present the Witness Oriented Asserted Location provenance framework. Our proposed work incorporates Asserted Location Proof (ALP) protocol and the OTIT model for secure location provenance. Witness ORiented framework implementation presented is a complete ready-to-deploy suite of applications, supporting all smart phones which are equipped with GPS tracker. Witness ORiented framework makes its presence more comfortable by featuring a web-based service provider, a desktop-based location authority server, an Android-based user app, a Google Glass-based client, and a desktop-based auditor. The system being presented is user centric without the requirement of having a centralized model. We have developed a secure protocol for WORAL on secure location proofs and augmented the protocol using secure location provenance preservation.

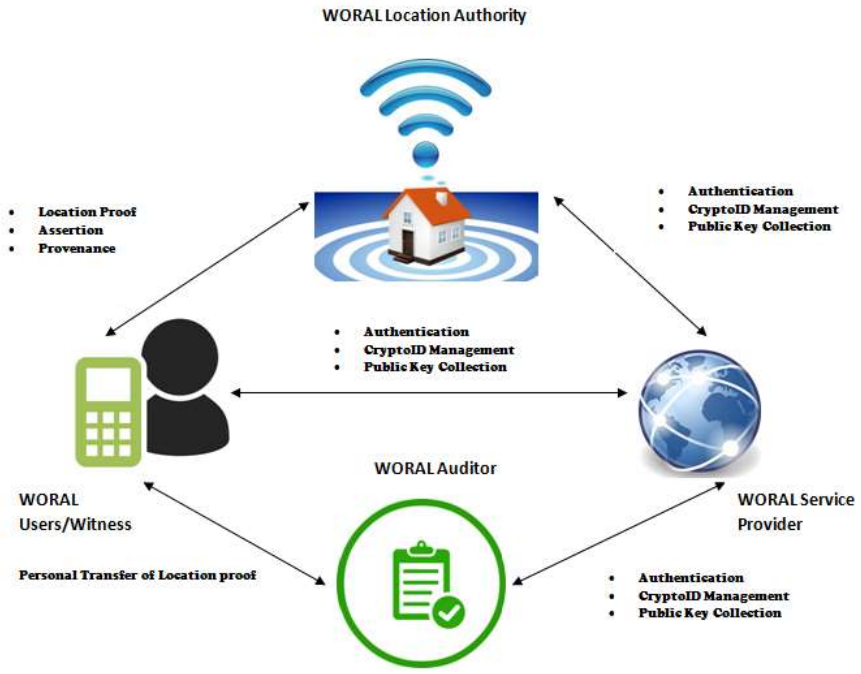

Fig-1: System Architecture of SLTMPW

Figure 1 above illustrates the system architecture of Secure Location Tracker for Mobile Devices by Providing Witness (SLTMPW), which includes location authority, Service Provider, User/Witness and Auditor. Figure 1 shows the overview of how the users, admin and location authority communicates and provide the services to the user. Witness here is mainly used to track the location of the user and verify it. Admin controls the activities of the user and witness. Auditor is then used to store the information provided by the user and witness.

WORAL Secure Location Provenance (WSLP) Algorithm

Step 1: Generating and Authenticating the Account

Location Authority, user and witness need to create an account to the Service Provider which must be uniquely distinguished.

Step 2: User Registration and Witness Registration

To provide his or her presence, user must get registered. Location Authority would maintain list of users who are interested to serve as witness.

Ureg= <CIDu, LPprov(LA)>

Wreg= <CIDw, PK(LA)>

ACK= <LA, Wi> where U-user, CID-CryptoID, ACK-Acknowledgment.

Step 3: Sharing of CryptoID and Key

Service Provider is responsible for sharing a public key pairs with Location Authority and users, which is used in further stages of process.

Step 4: IP address Generation

Generate an IP address for Location Authority which is used by the user and witness to create a TCP connection with Location Authority.

Unique ID is also created to the Location Authority to have a hold on the generated public key**.**

Step 5: Send Location Request

IP and the location requested by the user is sent to the service provider through location authority.

Location Proof Request will then be sent back to Location Authority.

Lreq= <LA, Wi>

Wi= <CIDu, Lprov($cur)>

Step 6: Acceptance of Location Request.

Witness registered, accepts/rejects the location request and sends proof to Location Authority.

Wi= <Lreq(Accept), Lprov>

Wi= <Lreq(Reject), Lprov(Failed)>

Wi= <CIDu, Lprov(cur)>

Step 7: Verification Request and Response Obtained.

Verification of the user's location is done by the witness as a proof of presence and deliver the response to Location Authority.

VFreq= <Lprov(V), ALprov(Wi), Tu>

Step 8: Generation of Witness List.

A list of users whose location is verified by the witness is then displayed in the verified list in the user's menu.

VL= <ALprov, ack, V(Lprov,ALprov), Tu>

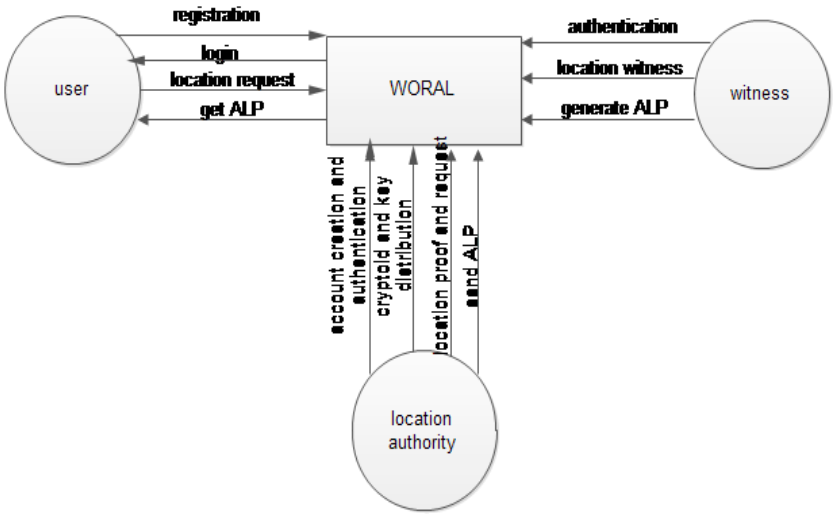

Fig-2: WORAL Dataflow Diagram

Figure 2 above depicts a system in terms of input data to the system, various processing carried out on this data and output data is generated by this system. There are four modules namely: User, Witness location authority and WORAL. User and witness register themselves to the WORAL app. Simultaneously, location authority authenticates the location proof of the user.

Advantages of proposed system:

Having introduced the concept of locations and asserted proof of presence widely used social networks and many other such user endorsed platforms have opportunities for implementing the proposed scheme adversely. Providing a proof of secure location with provenance preservation can be employed to form ad-hoc social networks and community networks. Introducing a secure, automated and antipathetic location proof generation scheme would be widely employed by many community users as the underlying mechanism for all those Location Based Services (LBS). Security, anti-hacking and fraud parameters can be highlighted and makes scheme to be used more widely.

RESULTS AND CONCLUSION

Accounting and reviewing of location evidence have been created. It is ready-to-deploy structure for reliable, secure, witness-oriented and source of origin protecting location proofs. Witness ORiented is based on the Asserted Location Proof protocol and deepen with provenance maintenance based on the OTIT model. The Witness ORiented structure provides the web-based service provider, desktop-based location authority server and an android based user application for the mobile app.

Fig-3: Account creation of Location Authority

Figure 3 above depicts the account creation of location authority which is stored in the database.

Fig-4: SignUp of User/Witness

Figure 4 above depicts the SignUp process of user/witness which includes the details of user/witness to be stored into the database.

Fig-5: Sending Location Request to Service Provider

Figure 5 above shows the details about the Crypto ID generated and the location provenance of the user.

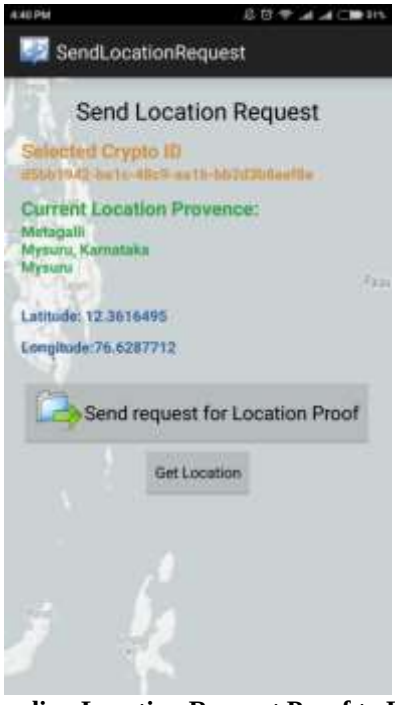

Fig-6: Sending Location Request Proof to Location Authority

Figure 6 above shows the details of user sending the location request to be witnessed to the location authority for the verification purpose.

Nowadays location-based services is a software-level service have created a need to control security and worthy of trust, reliable location method.

Ad-hoc social networks and community networks have enabled in storing the details in database. It has helped in tracking the origin of location for a given location authority. Co-located mobile devices which are in range mutually generate location proof and upload to the service provider and check for the number of users having same combination of public and private key to prevent certain attacks, like DoS attack, packet sniffing and also maintains load balancing.

Based on the users location privacy levels, user centric models except location proof request from the user, so the privacy level is highly maintained.

Request notification for witness by sending text messages or e-mails is included. We can store the information given by the user and the witness in the client, instead of storing it in a database in the server. The user can be tracked down even through the images of his current location. At a time one person may act as both user and witness for other users.

Clients can get more than one Crypto-ID's from the service provider which enables the seclusion by making many-to-one representation of the crypto-IDs to the original identity. Our work mainly includes the identification of the user along with the location. The user will be recognized for the temporal identities and later verified by auditor. The user has to use identities across the various locations including privacy of the user identity.

REFERENCES

1. Hasan, R., Khan, R., Zawoad, S., & Haque, M. (2015). **"**WORAL: A Witness Oriented Secure Location Provenance Framework for Mobile Devices**.** to appear *in IEEE Transactions on Emerging Topics in Computing (TETC) SI on Cyber Security.*
2. Khan, R., Zawoad, S., Haque, M. M., & Hasan, R. (2014**). "**Who, When, and Where? Location Proof Assertion for Mobile Devices**.** *DBSEC 2014 Vienna, Austria, July 14-16.*
3. Khan, R., Zawoad, S., Haque, M., & Hasan, R. (2014). **"**OTIT: Towards Secure Provenance Modeling for Location Proofs**",** in Proceedings of the 9th ACM Symposium on Information, *Computer and Communications Security (ASIACCS), Kyoto, Japan, June 2014. [pdf*]
4. Khan, R., Haque, M. M., & Hasan, R. (2013). "Modeling a Secure Supply Chain Integrity Preservation System"**,** *In Proceedings of IEEE International Conference on Technologies for Homeland Security*, Waltham, MA, November, 2013. [pdf].
5. Ananthanarayanan, G., Haridasan, M., Mohomed, I., Terry, D., & Thekkath, C. A. (2009).

"StarTrack: a framework for enabling track-based applications. *in Proc. of MobiSys, pp*. 207–220.
6. Brassil, J., Netravali, R., Haber, S., Manadhata, P., & Rao, P. (2012). "Authenticating a mobile device's location using voice signatures. *in Proc. of WiMob. IEEE, pp.* 458 –465.
7. Simmhan, Y. L., Plale, B., & Gannon, D. (2005). "A survey of data provenance in e-science. *SIGMOD Rec, 34*(3), 31– 36.
8. Bharathi, Haribhau, & Gaikwad. (2014). "APPLAUS- A privacy preserving location proof for lovation based service. *in international journal of computer science*.
9. Gonz´alez-Tablas, A. I., Ramos, B., & Ribagorda, A. (2003). "Path-stamps: A proposal for enhancing security of location tracking applications. *in Proc. of Ubiquitous Mobile Information and Collaboration Systems Workshop. Citeseer.*
10. Saroiu, S., & Wolman, A. (2009). "Enabling new mobile applications with location proofs. *in Proc. of HotMobile, 2009,* pp. 1–6.
11. Maduako, I. (2012). "*Wanna hack a drone? possible with geo-location spoofing*!" Online at http://geoawesomeness.com/?p=893.
12. Blumberg, A, J., & Eckersley, P. (2009). *"On locational privacy, and how to avoid losing it forever*. Online at https://www.eff.org/wp/ locational-privacy.
13. Hasan, R., Sion, R., & Winslett, M. (2009). "The case of the fake Picasso: Preventing history forgery with secure provenance. *in Proc. of FAST. USENIX Association, pp*. 1–12.
14. Zugenmaier, A., Kreutzer, M., & Kabatnik, M. (2001). "Enhancing applications with approved location stamps. *in Proc. of Intelligent Network Workshop. IEEE, p*. 140.
15. Senthil Guru, S., & Blessed Prince, P. (2013). "Survey on preserving privacy towards location proof" *in IJARCET*.