International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 9th June 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-4
Title: Empowering Protection – Safeguarding Location Proofs For Mobile Users.

Volume 06, Issue 04, Page No: 736-743.

Paper Authors

*** BOBBALA SRAVANI, T.NEETHA.**

* Brilliant Grammar School Educational Institutions.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

EMPOWERING PROTECTION – SAFEGUARDING LOCATION PROOFS FOR MOBILE USERS

[1]BOBBALA SRAVANI, [2]T.NEETHA.

[1] PG Scholar, Dept of CSE, Brilliant Grammar School Educational Institutions Group Of Institutions Integrated Campus, T.S, India

[2]Associate Professor, Dept of CSE, Brilliant Grammar School Educational Institutions Group Of Institutions Integrated Campus, T.S, India

ABSTRACT:

Location-based services are quickly becoming immensely popular. In addition to services based on users' current location, many potential services rely on users' location history, or their *spatial-temporal provenance*. Malicious users may lie about their spatial-temporal provenance without a carefully designed security system for users to prove their past locations. In this paper, we present the Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. Our prototype implementation on the Android platform shows that STAMP is low-cost in terms of computational and storage resources. Extensive simulation experiments show that our entropy-based trust model is able to achieve high collusion detection accuracy.

INTRODUCTION:

AS LOCATION-ENABLED mobile devices proliferate, location-based services are rapidly becoming immensely popular. Most of the current location-based services for mobile devices are based on users' current location. Users discover their locations and share them with a server. In turn, the server performs computation based on the location information and returns data/services to the users. In addition to users' current locations, there is an increased trend and incentive to prove/validate mobile users' past geographical locations. This opens a wide variety of new location-proof based mobile applications. Saroiu *et al.* described several such potential applications in [1]. Let us consider three examples: (1) A store wants to offer discounts to frequent customers. Customers must be able to show evidence of their repeated visits in the past to the store. (2) A company which promotes green

commuting and wellness mayreward their employees who walk or bike to work. The company may encourage daily walking goals of some fixed number of miles. Employees need to prove their past commuting paths to the company along with time history. This helps the company in reducing the healthcare insurance rates and move towards sustainable lifestyle. (3) On the battlefield, when a scout group is sent out to execute a mission, the commanding center may want every soldier to keep a copy of their location traces for investigation purpose after the mission.

Today's location-based services solely rely on users' devices to determine their location, e.g., using GPS. However, it allows malicious users to fake their STP information. Therefore, we need to involve third parties in the creation of STP proofs in order to achieve the integrity of the STP proofs. This, however, opens a number of security and privacy issues. First, involving multiple parties in the generation of STP proofs may jeopardize users' location privacy. Location information is highly sensitive personal data. Knowing where a person was at a particular time, one can infer his/her personal activities, political views, health status, and launch unsolicited advertising, physical attacks or harassment [7]. Therefore, mechanisms to preserve users' privacy and anonymity are mandatory in an STP proof system. Second, authenticity of STP proofs should be one of the main design goals in order to achieve integrity and non-transferability of STP proofs. Moreover, it is possible that multiple parties collude and create fake STP proofs. Therefore, careful thought must be given to the countermeasures against collusion attacks. In this paper, we propose an STP proof scheme named Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP). STAMP aims at ensuring the integrity and non-transferability of the STP proofs, with the capability of protecting users' privacy. Most of the existing STP proof schemes rely on wireless infrastructure (e.g., WiFi APs) to create proofs for mobile users. However, it may not be feasible for all types ofapplications, e.g., STP proofs for the green commuting and battlefield examples certainly cannot be obtained from wireless APs. To target a wider range of applications, STAMP is based on a distributed architecture. Co-located mobile devices mutually generate and endorse STP proofs for each other, while at the same time it does not eliminate the possibility of utilizing wireless infrastructures as more trusted proof

generation sources. In addition, in contrast to most of the existing schemes which require multiple trusted or semi-trusted third parties, STAMP requires only a single semi-trusted third party which can be embedded in a Certificate Authority (CA). We design our system with an objective of protecting users' anonymity and location privacy. No parties other than verifiers could see both a user's identity and STP information (verifiers need both identity and STP information in order to perform verification and provide services). Users are given the flexibility to choose the location granularity level that is revealed to the verifier. We examine two types of collusion attacks: (1) A user who is at an intended location masquerades as another colluding user and obtains STP proofs for . This attack has never been addressed in any existing STP proof schemes. (2) Colluding users mutually generate fake STP proofs for each other. There have been efforts to address this type of collusion. However, existing solutions suffer from high computational cost and low scalability. Particularly, the latter collusion scenario is in fact the challenging *Terrorist Fraud* attack [8], which is a critical issue for our targeted system, but none of the existing systems has addressed it. We integrate the Bussard-Bagga distance bounding protocol [9] into STAMP to protect our scheme against this collusion attack. Collusion scenario (1) is hard to prevent without a trusted third party. To make our system resilient to this attack, we propose an entropy-based trust model to detect the collusion scenario. We implemented STAMP on the Android platform and carried out extensive validation experiments. The experimental results show that STAMP requires low computational overhead.

RELATED WORK:

The notion of unforgeable location proofs was discussed by Waters *et al.* [10]. They proposed a secure scheme which a device can use to get a location proof from a location manager. However, it requires users to know the verifiers as a prior. Saroiu *et al.* [1] proposed a secure location proof mechanism, where users and wireless APs exchange their signed public keys to create timestamped location proofs. These schemes are susceptible to collusion attacks where users and wireless APs may collude to create fake proofs. VeriPlace [2] is a location proof architecture which is designed with privacy protection and collusion resilience. However, it requires three different trusted entities to provide security and privacy protection: a TTPL (Trusted Third Party for managing Location

in formation), a TTPU (Trusted Third Party for managing User information) and a CDA (Cheating Detection Authority). Each trusted entity knows either a user's identity or his/her location, but not both. VeriPlace's collusion detection works only if users request their location proofs very frequently so that the long distance between two location proofs that are chronologically close can be considered as anomalies. This is not a realistic assumption because users should have the control over the frequency of their requests.

EXISTING SYSTEM: In the existing system there is a lot of volunteers are needed and also consuming lot of time. Location privacy is an extremely important factor that needs to be taken into consideration when designing any location based systems. Revealing both identity and location information to an untreated party poses threats to a mobile users. Today's location-based services solely rely on users' devices to determine their location, e.g., using GPS. However, it allows malicious users to fake their STP information.

Therefore, we need to involve third parties in the creation of STP proofs in order to achieve the integrity of the STP proofs. This, however, opens a number of security and privacy issues. First, involving multiple parties in the generation of STP proofs may jeopardize users' location privacy.

Location information is highly sensitive personal data. Knowing where a person was at a particular time, one can infer his/her personal activities, political views, health status, and launch unsolicited advertising, physical attacks or harassment. Authenticity of STP proofs should be one of the main design goals in order to achieve integrity and non-transferability of STP proofs. Moreover, it is possible that multiple parties collude and create fake STP proofs. There are disadvantages in existing system they are

- Mechanisms to preserve users' privacy and anonymity are not provided.
- Possibility of multiple parties to collude and create fake STP proofs.
- Revealing both identity and location information to an untreated party poses threats to a mobile users.
- Lack of accuracy. It is very burden to Users.
- Lot of paper works.

PROPOSED SYSTEM: In this paper, we propose an STP proof scheme named Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP). STAMP aims at ensuring the integrity and non-transferability of the STP proofs, with the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

capability of protecting users' privacy. Most of the existing STP proof schemes rely on wireless infrastructure to create proofs for mobile users. However, it may not be feasible for all types of applications. Advantages of our system are:

- A distributed STP proof generation (STAMP) is introduced to achieve integrity and non-transferability of STP proofs.
- STAMP is designed to maximize users' anonymity and location privacy. Users are given the control over the location granularity of their STP proofs.
- STAMP is collusion-resistant. The system is integrated into STAMP to prevent a user from collecting proofs on behalf of another user. An entropy-based trust model is proposed to detect users mutually generating fake proofs for each other.
- A security analysis is presented to prove STAMP achieves the security and privacy objectives.
- A prototype application is implemented on the Android platform. Experiments show that STAMP requires preferably low computational time and storage.
- Reduce time for searching the route between the locations. Gives accurate details about the current location.
- User friendly. Reduces paper works. Easy communication between user and the admin.

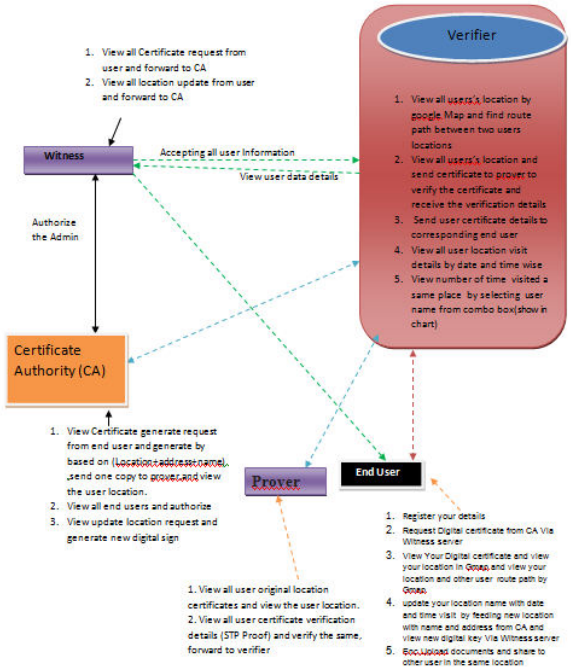

Fig: System Architecture

IMPLEMENTATION: Every implementation is having its own uses. We discussed about the implementation of opinion mining in this paper. They are:

User Details: The admin can view the details of the registered user .From that he can access or perform further processing that he wants to do.

Location Details: The user share their location details to admin from there admin can view the location with the time and date that the user has shared from there the admin will verify his distance from the office and send him a gift voucher to encourage him to

come by walk to the office there by reducing the health insurance issues for the office. In knowing the details the admin has to decrypt the details because it will come as encrypted by the user with a password. If only the password is known means the admin can decrypt the details about the user location which is known as the privacy preserving location proof sharing. For decryption he needs a password which is used by the user, the user sends he password to the user through email, from there admin can view the password and utilize it for decryption.

Sending SMS: By verifying the distance in the Google map the admin will come to the conclusion that who are all eligible for the gift voucher and send message to the users.

My Location: In the My location the user will find his current location in the Google map on single button click helps him to find his current location.

Finding Route: Finding route the user can find his route with distance to reach his destination along with the time taken to reach the distance.

Sharing Location: In the sharing location the user will share his location to the user .Where sharing is made privacy. This means the user share his location encrypted with a password. And if only the password is known by the admin, he can decrypt the user location which is known as the privacy preserving location sharing.

Sharing Password: For sharing password the user will share his password to the admin through mail. The admin will utilize the password from the mail.

CONCLUSION: In this paper we have presented STAMP, which aims at providing security and privacy assurance to mobile users' proofs for their past location visits. STAMP relies on mobile devices in vicinity to mutually generate location proofs or uses wireless APs to generate location proofs. Integrity and non-transferability of location proofs and location privacy of users are the main design goals of STAMP.

REFERENCES:

1. S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proc. ACM HotMobile*, 2009, Art. no. 3.
2. W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture," in *Proc. ACM GIS*, 2010, pp. 23–32.
3. Z.Zhu and G. Cao, "Towards privacy-preserving and

colluding-resistance in location proof updating system," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 51–64, Jan. 2011.

4. N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM WiSe*, 2003, pp. 1–10.
5. R. Hasan and R. Burns, "Where have you been? secure location provenance for mobile devices," *CoRR* 2011.
6. B. Davis, H. Chen, and M. Franklin, "Privacy preserving alibi systems," in *Proc. ACM ASIACCS*, 2012, pp. 34–35.
7. I. Krontiris, F. Freiling, and T. Dimitriou, "Location privacy in urban sensing networks: Research challenges and directions," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 30–35, Oct. 2010.
8. Y. Desmedt, "Major security problems with the 'unforgeable' (feige)-fiat-shamir proofs of identity and how to overcome them," in *Proc. SecuriCom*, 1988, pp. 15–17.
9. L. Bussard and W. Bagga, "Distance-bounding proof of knowledge to avoid real-time attacks," in *Security and Privacy in the Age of Ubiquitous Computing*. New York, NY, USA: Springer, 2005.
10. B. Waters and E. Felten, "Secure, private proofs of location," Department of Computer Science, Princeton University, Princeton, NJ, USA, Tech. Rep., 2003.
11. X. Wang *et al.*, "STAMP: Ad hoc spatial-temporal provenance assurance for mobile users," in *Proc. IEEE ICNP*, 2013, pp. 1–10.
12. A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudonymity-a proposal for terminology," in *Designing Privacy Enhancing Technologies*. New York, NY, USA: Springer, 2001.
13. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 370–380, Feb. 2006.
14. S. Halevi and S. Micali, "Practical and provably-secure commitment schemes from

collision-free hashing," in *Proc. CRYPTO*, 1996, pp. 201–215.

15. I. Damgård, "Commitment schemes and zero- knowledge protocols," in *Proc. Lectures Data Security*, 1999, pp. 63–86.
16. I. Haitner and O. Reingold, "Statistically-hiding commitment from any one-way function," in *Proc. ACM Symp. Theory Comput.*, 2007, pp. 1–10.
17. D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in *Proc. IEEE MASS*, 2005.
18. J. Reid, J. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *Proc. ACM ASIACCS*, 2007, pp. 204–213.
19. C. Kim, G. Avoine, F. Koeune, F. Standaert, and O. Pereira, "The Swiss-knife RFID distance bounding protocol," in *Proc. ICISC*, 2009, pp. 98–115.
20. H. Han *et al.*, "Senspeed: Sensing driving conditions to estimate vehicle speed in urban environments," in *Proc. IEEE INFOCOM*, Apr. 2014, pp.