International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN: 2456-3307

Facilitating Privacy Conserving Position Proofs for Mobile Users

B. Sreedhar[1]

[1]MCA, Sri Padmavathi College Of Computer Sciences and Technology, Tiruchanoor, Tirupathi, Andhra Pradesh, India

ABSTRACT

With the popularity of social media (e.g., Facebook and Flicker), users can easily share their check-in records and photos during their trips. Location-based services are quickly changing into vastly popular. Additionally to services supported users' current location, several potential services suppose users' location history, or their spatial-temporal provenance. Malicious users could laze their spatial-temporal provenance while not a fastidiously designed security system for users to prove their past locations. In this paper, we present the Spatial-Temporal root age Assurance with Mutual Proofs theme. It is intended for ad-hoc mobile users generating location proofs for every different in a distributed setting. However, it will simply accommodate trusted mobile users and wireless access points. Spatial-Temporal rootage Assurance with Mutual Proofs ensures the integrity and non-transferability of the situation proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptologic keys moreover as guard users against collusion by a light-weight entropy-based trust analysis approach. Our example implementation on the automaton platform shows that Spatial-Temporal rootage Assurance with Mutual Proofs is affordable in terms of machine and storage resources. Intensive simulation experiments show that our entropy-based trust model is ready to realize high collusion detection accuracy.

Keywords : Location Proof, Privacy, Spatial-Temporal Provenance, Trust.

I. INTRODUCTION

Location-based social network (LBSN) services permit users to perform arrival and share their arrival information with their friends. Above all, once a user is travelling, the check-in information are in truth a travel route with some photos and tag info. As a result, an enormous range of routes are generated, that play a vital role in several well-established analysis areas, like quality prediction, urban designing and traffic management.

As location-enabled mobile devices proliferate, location- based services are rapidly turning into vastly popular. Most of these location-based services for mobile devices are supported users' current location. Users discover their locations and share them with a server. In turn, the server performs computation supported the placement info and returns data/services to the users. Additionally to users' current locations, there is an accumulated trend and incentive to prove/validate mobile users' past geographical locations. This opens a wide variety of latest location-proof primarily based mobile applications.

In existing system we study the travel route recommendation problem. We've developed a KRTR framework to recommend travel routes with a selected vary and a group of user preference keywords. These travel routes are related to all or partial user preference keywords, and are suggested based on (i) the attractiveness of the POIs it passes, (ii) visiting the POIs at their corresponding correct arrival times, and (iii) the routes generated by authoritative users. We propose a novel keyword extraction module to spot the linguistics meaning and match the activity of routes, and have designed a route reconstruction algorithmic rule to combination route segments into travel routes in accordance with query range and period of time. We tend to leverage score functions for the three said options and adapt the representative Skyline search rather than the normal top-k recommendation system.

In this paper we've bestowed Spatial-Temporal provenance Assurance with Mutual Proofs, that aims at providing security and privacy assurance to mobile users' proofs for their past location visits. Spatial-Temporal provenance Assurance with Mutual Proofs depends on mobile devices in section to reciprocally generate location proofs or uses wireless APs to come up with location proofs. Integrity and non-transferability of location proofs and site privacy of user's area unit the main style goals of Spatial-Temporal provenance Assurance with Mutual Proofs. We've specifically prohibited 2 collusion scenarios: P-P collusion and P-W collusion. To safeguard against P-P collusions, we integrated the Bussard-Bagga distance bounding protocol into the look of Spatial-Temporal provenance Assurance with Mutual Proofs. To observe P-W collusion, we projected associate entropy-based trust model to judge the trust level of claims of the past location visits. Our security analysis shows that Spatial-Temporal provenance Assurance with Mutual Proofs achieves the safety and privacy objectives. Our implementation on robot smart phones indicates that low process and storage resources area unit needed to execute Spatial-Temporal provenance Assurance with Mutual Proofs.

II. SCHEME

A distributed STP proof generation and verification protocol is introduced to achieve integrity and non-transferability of STP proofs. No additional trusted third parties are required except for a semi-trusted CA. Spatial-Temporal provenance Assurance with Mutual Proofs scheme 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 Bussard-Bagga distance bounding protocol is integrated into Spatial-Temporal provenance Assurance with Mutual Proofs scheme 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. Spatial-Temporal provenance Assurance with Mutual Proofs scheme uses a entropy-based trust model to guard users from prover-witness collusion. This model also encourages witnesses against selfish behavior. Modifications to STAMP to facilitate the utilization of stationary wireless infrastructure APs or trusted mobile users are presented. 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 Spatial-Temporal provenance Assurance with Mutual Proofs scheme requires preferably low computational time and storage. Simulation experiments validate that our entropy-based trust model is able to achieve over 0.9 collusion detection accuracy with fairly high percentage of colluding attackers.

III.CONCLUSION

In this paper we've presented Spatial-Temporal provenance Assurance with Mutual Proofs scheme, that aims at providing security and privacy assurance to mobile users' proofs for their past location visits. Spatial-Temporal provenance Assurance with Mutual Proofs scheme depends on mobile devices in neck of the woods to reciprocally generate location proofs or uses wireless APs to come up with location proofs. Integrity and non-transferability of location proofs and placement privacy of users square measure the main style goals of Spatial-Temporal provenance Assurance with Mutual Proofs scheme. We've specifically addressed 2 collusion scenarios: P-P collusion and P-W collusion. to safeguard against P-P collusions, we integrated the Bussard-Bagga distance bounding protocol into the planning of STAMP. To discover P-W collusion, we projected an entropy-based trust model to judge the trust level of claims of the past location visits. Our security analysis shows that Spatial-Temporal provenance Assurance with Mutual Proofs scheme achieves the protection and privacy objectives. Our implementation on golem smart phones indicates that low machine and storage resources square measure needed to execute Spatial-Temporal provenance Assurance with Mutual Proofs scheme. In depth simulation results show that our trust model is in a position to realize a high balanced accuracy with applicable selections of system parameters.

IV. CONCLUSION

[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.