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 13th July 2017. Link :

http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-5

Title: Stamp: Enabling Privacy-Preserving Location Proofs For Mobile Users.

Volume 06, Issue 05, Page No: 1759 - 1763.

Paper Authors

*** PELLURI SAI PASYANTHI, B KRISHNA.**

* Dept of CSE, Visakha Institute of Engineering& Technology College.

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

STAMP: ENABLING PRIVACY-PRESERVING LOCATION PROOFS FOR MOBILE USERS

***PELLURI SAI PASYANTHI, **B KRISHNA**
*PG Scholar, Dept of CSE, Visakha Institute of Engineering& Technology College
Vizag (Dt),A.P India.
**Associate Professor, Dept of CSE, Visakha Institute of Engineering& Technology College
Vizag (Dt),A.P, India.
saipasyanthi@gmail.com vietmtechcse@gmail.com

ABSTRACT:
Nowadays location based mostly services area unit quickly turning into common. Several services that area unit supported user’s location can even use the user’s location history or their spatial-temporal place of origin. It uses GPS technology international Positioning System (GPS) could be a satellite-based navigation system created of a network of various satellites. Malicious users could slug their spatial-temporal place of origin while not a rigorously designed security system for users to prove their past locations. associate degree word form STAMP stands for abstraction Temporal place of origin Assurance with Mutual Proofs. Essentially STAMP is meant for ad-hoc mobile users generating location proofs for every different in a very distributed setting. thus it will simply accommodate trustworthy mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the situation proofs and protects user’s privacy. A semi-trusted certification Authority is employed to distribute cryptologic keys in addition as guard users against collusion by light-weight entropy based mostly trust analysis approach. STAMP is affordable in terms of procedure and storage resources. This protocol is meant to maximise user’s namelessness and site privacy. Here users area unit given the management over the situation graininess of their standard atmosphere proofs. STAMP is collusion resistant. associate degree entropy-based trust model is projected to notice users reciprocally generating pretend proofs for every different.

KEY WORDS*:* Global Positioning System, Location Proof, Privacy, Spatial-Temporal beginning

I. INTRODUCTION

Today’s several location-based services think about user’s location supported their devices exploitation GPS. It permits some malicious users to faux their atm info. so there's have to be compelled to accomplish integrity of atm proofs. essentiallyatm stands for abstraction Temporal root wherever abstraction suggests that one thing concerning area, Temporal suggests that one thing concerning time and last however not the smallest amount root is expounded to history of one thing. Most of the present atm proof schemes think about wireless infrastructure (e.g. Wi-Fi APs) to form proofs for mobile users. this method proposes associate degree atm proof theme named Spatial-Temporal root Assurance with Mutual proofs (STAMP). STAMP aims at guaranteeing the integrity and non-transferability of the atm proofs, with the aptitude of protective users' privacy. However, it's going to not be possible for every type of applications, e.g., atm proofs for the inexperienced commutation and battleground examples definitely can't be obtained from wireless APs. to focus on a wider vary of applications, STAMP relies on a distributed design. Following figure shows the system design. essentially it works exploitation completely different devices. There ar four sorts of entities:

1) Prover: A prover may be a mobile device that tries to get standard pressure proofs at a precise location.

2) Witness: A witness may be a device that is in proximity with the prover Associate in Nursingd is willing to form an standard pressure proof for the prover upon receiving his/her request. The witness will be untrusted or trustworthy , and also the trustworthy witness will be mobile or stationary (wireless APs). Collocated mobile users area unit untrusted.

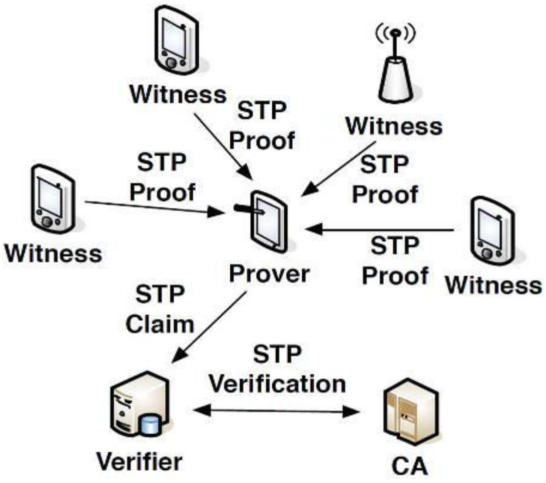

Fig. 1: An illustration of system architecture

3) Verifier: A voucher is that the party that the prover needs to point out one or a lot of standard pressure proofs to and claim his/her presence at a location at a specific time.

4) Certificate Authority (CA): The CA may be a semi-trusted server (untrusted for privacy protection, see Section IV-C for details) that problems, manages cryptanalytic credentials for the opposite parties. CA is additionally to blame for proof verification and trust analysis. A prover and a witness communicates with one another via Bluetooth or Wi-Fi in impromptu mode. The proof generation system of prover is bestowed a listing of obtainable witnesses. once there area unit multiple witnesses willing to co-operate, the prover initiate protocol with them consecutive. standard pressure claims area unit sent to verifiers from provers via a LAN or web, and verifiers area unit assumed to possess web reference to CA. every user will act as a prover or a witness, betting on their roles at the instant. this method assumes the identity of a user is certain with his/her public key, that is certified by CA. Users have distinctive public/private key pairs, that area unit established throughout the user registration with CA and hold on on users' personal devices..

II. LITERATURE SURVEY

A. Enabling new mobile applications with location proofs. [1]

Author introduces location proofs – an easy mechanism that permits the emergence of mobile applications that need “proof” of a user’s location. It permits mobile devices to firmly prove their current and past locations. Author presents a concrete protocol that is implementable over Wi-Fi during which APs issue location proofs to mobile devices. A location proof may be a piece of information that certifies a geographical location. Access points (APs) imbed their geographical location in location proofs, that ar then transmitted to selected recipient devices. A location proof has 5 fields: associate degree institution, a recipient, a timestamp, a geographical location, and a digital signature. this method describes many potential applications wherever location proofs play a central role in sanctionative them like store discounts for loyal customers, inexperienced computing, reducing fraud on auction websites, location-restricted content delivery and police investigations. this method has four security properties like integrity, non-transferability, unforgeability, privacy.

B. VeriPlace: A privacy-aware location proof architecture [2]

This system known four challenges in planning a location proof design and addressed them in VeriPlace. this technique illustrated however science techniques will aid in conserving user privacy and protective system security. VeriPlace system may be a location proof design that is meant with privacy protection and collusion resilience. this technique needs 3 totally different trusty entities to supply 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 trusty entity is aware of either a user's identity or his/her location, however not each. VeriPlace's collusion detection works given that users request their location proofs terribly oft so the long distance between 2 location proofs that area unit chronologically shut is thought of as anomalies. There area unit 2 advantages of this technique like user privacy and cheating detection. Author mentioned very well regarding four security challenges like privacy, security, flexibility, deployability.

C. Towards privacy-preserving and colluding-resistance in location proof updating system [3]

Author proposes a system naming a privacy conserving location proof change system known as APPLAUS. during this system Bluetooth enabled mobile devices reciprocally generate location proofs and transfer to the placement proof server. It represents a theme that depends on each location proofs from wireless APs and witness endorsements from Bluetooth-enabled mobile peers. APPLAUS system may be able to offer time period location proofs effectively. It preserves supply location privacy and it's collusion resistant. Author conjointly developed a user centrical location privacy model during which individual users assess their location privacy levels in real time and user will decide whether or not and once to simply accept a location privacy levels. Betweenness ranking based mostly and correlation clustering-based approaches for outlier detection also are developed here to subsume the colluding attacks,

D. LINK Location verification through immediate neighbors knowledge

For each users location claim, a centralized Location Certifcation Authority (LCA) receives variety of verification messages from neighbors contacted by the claimer victimisation short-range wireless networking love Bluetooth. The LCA decides whether or not the claim is authentic or not supported spatio-temporal correlation between the users, trust scores related to every user, and historical trends of the trust scores. It conjointly detects attacks involving teams of colluding users. Privacy and security analysis the system conjointly monitor users and needs their credentials to manifest the proof. In different terms, users aren't anonymous concerning the system.

E. Where have you been? secure location provenance for mobile devices

Author proposes a theme that depends on each location proofs from wireless APs and witness endorsements from Bluetooth-enabled mobile peers, so no users will forge proofs while not colluding with each wireless APs and different mobile peers at identical time A secure location-based service needs that a mobile user certifies his position before gaining access to a resource. Currently, most of the present solutions addressing this issue assume a trustworthy third party that may vouch for the position claimed by a user. However, as computation and communication capacities become omnipresent with the massive scale adoption of smartphones by people, we have a tendency to propose to leverage on these resources to unravel this issue during a cooperative and personal manner.

F. Location privacy in urban sensing networks: Research challenges and directions

Location info is extremely sensitive personal knowledge. Knowing wherever someone was at a specific time, one will infer his/her personal activities, political beliefs, health standing, and launch unsought advertising, physical attacks or harassment of these location-sensitive applications need users to prove that they extremely area unit (or were) at the claimed location. though most mobile users have devices capable of discovering their locations, they lack a mechanism to prove their current or past locations to applications and services III.

CONCLUSION

In the projected system STAMP protocol is painted to produce security and privacy assurance to mobile users proofs for his or her past location visits. STAMP 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 users area unit the most style goals of STAMP.

ACKNOWLEDGEMENT

I would wish to take this chance to specific profound feeling and deep reference to professor. Bharati Kale, for her exemplary steering, valuable feedback and constant encouragement throughout the period of this work. Her valuable suggestions carry up my work. Her perceptive criticism unbroken American state operating to create this analysis add far better manner. operating below her is a particularly knowledgeable expertise on behalf of me.

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. 727–735.