International Journal for Modern Trends in Science and Technology
Volume: 03, Special Issue No: 02, March 2017
ISSN: 2455-3778
http://www.ijmtst.com

A Neoteric Approach for Enabling Privacy - Preserving Location Claims for Mobile Users

B.Nalini[1] | A.Rojarani[2] | V.Bhanu Prasuna[3] | L.Priyadarsini[4]

[1,2,3,4]Department of IT, Andhra Loyola Institute of Engineering & Technology, Vijayawada, Andhra Pradesh, India.

To Cite this Article
B.Nalini, A.Rojarani, V.Bhanu Prasuna and L.Priyadarsini, "A Neoteric Approach for Enabling Privacy - Preserving Location Claims for Mobile Users", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Special Issue 02, 2017, pp. 42-46.

ABSTRACT

Now-a-days the most popular services islocation based services when comparing with other services .Location based services are mostly used by the users either for the location history or their Spatial – Temporal Provenance (STP) based on their current location STP are hidden by the awful users as they don't have a perfectly designed security system to witness their earlier location . In this location we have introduced a scheme called "STAMP (Spatial temporal provenance assurance with mutual proof)". It is designed to distribute settings where mobile users generate their own location witness for each others. Wireless access points and trusted mobile users are accommodated easily by STAMP. It ensures integrity and non- transferability are achieved by STAMP. A light weight entropy based trusty evaluating approach is used to safeguard users against collusion and distributed cryptographic keys are generated by semi-trusted Certification Authority. A high collision detection accuracy is achieved by extensive simulation experiments that proves entropy based trusted model.NEOTERIC is low cost interms of computational in storage resources. It is easily accomodate trusted mobile users and wireless access points.

I. INTRODUCTION

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 theirlocations and share them with a server. In turn, the server performscomputation 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.In this paper, we consider the two terms interchangeable. We prefer "STP proof" because it indicates that such a proof is intended for past location visits with both spatial and temporalinformation. Today's location-based services rely on users' devices to determine their location, e.g., using GPS. 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. Therefore we need to involve third party in need to creation of STP proofs inorder to achieve integrity of STP In this it shows about the information highly sensitive data an user/employee.knowing where a person was at a particular time one cannot interfere his/her personal activities,health status ,location status .In this paper ,we propose an STP

Proof i.e Latitude and Longitude of a Location of an employee this aims at ensuring the integrity and non-transferability of the STP proofs with the capability of protecting users security The *contributions* of this paper can be summarized as:

1) A distributed STP proof generation and verification and a protocol NEOTERIC APPROACH is introduced to achieve integrity and nontransferabilityof STP proofs. No additional trusted third parties are required except for a semi-trusted CA.

2) NEOTERIC APPROACH is designed to maximize users' anonymity and location privacy. Users are given the control over the locationgranularity of their STP proofs.

3) STAMP is collusion-resistant. The Bussard-Bagga distance bounding protocol 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.

4)STAMP uses a entropy-based trust model to guard users from prover-witness collusion. This model also encourages witnesses against selfish behavior.

5) Modifications NEOTRIC APPROACH STAMP to facilitate the utilization of stationarywireless infrastructure APs or trusted mobile users are presented.

6) A security analysis is presented to prove STAMP achieves the security and privacy objectives.

7) A prototype application is implemented on the Android platform. Experiments show that STAMP requires preferably low computational time and storage.

8) Simulation experiments validate that our entropy-based trust model is able to achieve over 0.9 collusion detection accuracy with fairly high percentage of colludingattackers.The remaining paper is organized as follows: Section II discusses related work. Section III describes our system model andin Section IV, we discuss the security requirements in detail and describe the threat model of this work. In Section V, we present the details of the STAMP protocol. Section VI provides an overview of how STAMP can be practically used in number of scenarios including trusted mobile users and wireless APs. security analysis of STAMP against different types of attacks is provided in Section VII. In Section VIII, we describe our implementation and simulation and present our experimental results on the performance evaluation. We give a discussion and outline our future work in Section IX. Finally, Section X concludes All the above systems are centralized, that is, they all require central infrastructures (wireless APs) to act as the location authorities and generate location proofs. However, we want to designa framework that can also work for distributed scenario where users are far from any trusted AP.

II. RELATED WORK

In Davis *et al.*'s alibi system , their private corroborator relies on mobile users within proximity to createalibi's (i.e., location proofs) for each other. The security and privacy of the system is achieved based on cryptographic key i.easyymeric algorithm commitment scheme. In order to protect privacy, the knowledge of private information is separately distributed to three parties: a location proof server, a CA and the verifier. Periodically changed pseudonyms are used by the mobile devices to protect their real identities from each other, and from the location proof server. We believe the location proof server is foraccomplishing the goals.APPLAUS is a location proof system that is based on co-located mobile devices by mutually generating location proofs among three parties in a distributed system a location proof server, a CA, and the verifier. These three are essential to hide the identity from each other. We believe the location proof server is Good for accomplishing all the goals incurs high operational overhead due to the requirement for highly cautious management and scheduling. The collusion detection in this is based on ranking and correlation clustering. this needs users to submit their location proofs right after by generating .if there is no internet Connection . then these approaches will cost more in computing power to run the detection and their successful detection ratio is highonly when the percentage of the colluding attackers israther low . All the above systems are centralized, that is, they all requirecentral infrastructures (wireless APs) to act as the location authoritiesand generate location proofs. However, we want to designa framework that can also work for distributed scenariosencounters is specific to the application scenarios) and he/she
intends to make a claim about his/her past STP to the verifier, theSTP claim and verification phase takes place between the proverand the verifier. A part of the verification job has to be doneby CA.

Therefore, communication between the verifier and CAhappens in the middle of the STP claim and verification phase.

In Fig. 2, the two arrowed lines in red color represent thelatter two stages of the Bussard-Bagga protocol. These stages require multiple interactions between the two involved parties,and thereby are represented by doubly arrowed lines. The preparationstage of the Bussard-Bagga protocol does not need to beexecuted for every STP proof generation and thus is not shown.Users could run the preparation stage before each STP proofcollection event or pre-compute and store several sets of the bitcommitments and primitives, and randomly choose one set of

III. SYSTEM MODEL

Wireless infrastructure may not be available everywhere and hence a system based on wireless APs creating STP proofs would not be feasible for all scenarios. In addition, the deployment cost would be high if we require a large number of wireless APs to have the capability of generating STP proofs. Therefore, we think a distributed STP proof architecture, i.e., mobile users obtaining STP proofs from nearby mobile peers, would be more feasible and appropriate for a wider range ofapplications. We design a generic decentralized protocol, and then show how it can work well for centralized case also.Fig. 1 illustrates the architecture of our system. There are four of entities based on their roles:

• **Prover:** A *prover*is a mobile device which tries to obtain STP proofs at a certain location.

• **Witness:** A *witness* is a device which is I n proximity with the prover and is willing to create an STP proof for the prover upon receiving his/her request. The witness can be untrusted or trusted, and the trusted witness can be mobile or stationary (wireless APs). Collocated mobile users areuntrusted.

• **Verifier**: A *verifier* is the party that the prover wants to show one or more STP proofs to and claim his/her presence at a location at a particular time.

• **Certificate Authority (CA***)*: The *CA* is a semi-trusted server (untrusted for privacy protection, see Section IV-C for details) which issues, manages cryptographic credentials for the other parties. CA is also responsible for proof verification protocol. The proof generation system of prover is presented alist of available witnesses. When there are multiple witnesses willing to cooperate, the prover initiate protocol with them sequentially. STP claims are sent to verifiers from provers via a LAN or Internet, and verifiers are assumed to have Internet connectionwith CA. Each user can act as a prover or a witness,depending on their roles at the moment. We assume the identity of a user is bound with his/her public key, which is certified by CA. Users have unique public/private key pairs, which are established during the user registration with CA and stored on users' personal devices.

•**Witness**: A *witness* is a device which is in proximity with the prover and is willing to create an STP proof for the prover upon receiving his/her request. The witness can be untrusted or trusted, and the trusted witness can be mobile or stationary(wireless APs). Collocated mobile users areuntrusted.

• **Verifier:** A *verifier* is the party that the prover wants to show one or more STP proofs to and claim his/her presence at a location at a particular time.

• **Certificate Authority (CA***)*: The *CA* is a semi-trusted server (untrusted for privacy protection, see Section IV-C for details) which issues, manages cryptographic credentials for the other parties. CA is also responsible for proof verification protocol. The proof generation system of prover is presented alist of available witnesses. When there are multiple witnesses willing to cooperate, the prover initiate protocol with them sequentially. STP claims are sent to verifiers from provers via a LAN or Internet, and verifiers are assumed to have Internet connectionwith CA. Each user can act as a prover or a witness,depending on their roles at the moment. We assume the identity of a user is bound with his/her public key, which is certified by CA. Users have unique public/private key pairs, which are established during the user registration with CA and stored on users' personal devices.

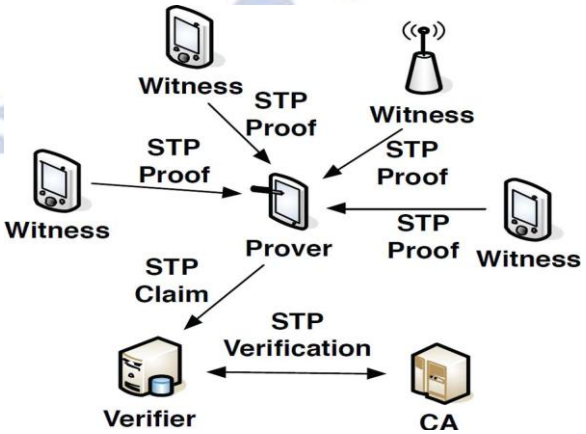


Fig. 1. An illustration of system architecture

Aprover and a witness communicates with each other via Bluetooth or WiFi in ad hoc mode. A peer discovery mechanism for finding the exact location of an employee

IV. REQUIREMENTS AND CHALLENGES

The important issues and design challenges involved,in order to give an intuition of our objectives of constructing the protocol.

A. Security

The security of STP proofs are two fold: *integrity* and*non-transferability* . The integrity property requires that no proveri.e employee/user can create fake STP proofs by himself/herself or by collaborating with one or more other untrusted parties in the system. The non-transferability property requires that no prover can claim the ownership of another prover's legitimate STP proofs.

B. Privacy

Anonymity: 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 untrusted party poses threats to a mobile users. First, a prover should be able to hide his/her identity from a witness. In addition, it is not only the prover's anonymity that we should pay attention to, a witness's anonymity shouldalspreserved. Since a witness who agrees tocreate an STP revealed to the verifier.

C. Threat Model

Prover*:* A malicious prover seeks to create fake STP proofs.Hereprover can update hi current location through server to the certified authority.

Witness*:* A malicious witness's goals include acquiring a prover's identity information and repudiating an STP proof that is generated by him/her.

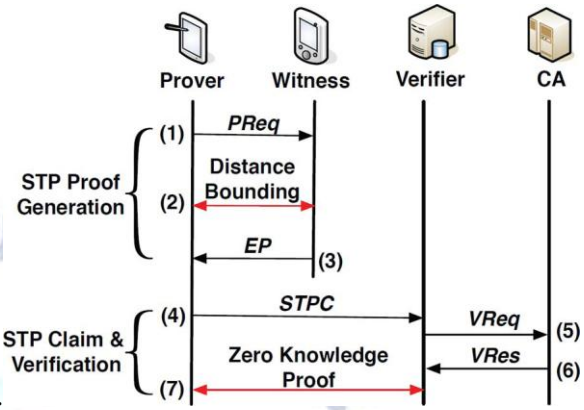
Verifier:A verifier is often a service provider or an authority here verifier is nothing but the certified authority i.e admin can check nthe particular employee/user details.

V. THE STAMP SCHEME

A. Preliminaries

1)Location Granularity Levels*:* We assume there are granularity levels for each location, which can be denoted by ,L1,L2……,Ln where L1 represents the finest locationgranularity (e.g., an exact Geo coordinate), and represents the most coarse location granularity (e.g., a city).

2) Cryptographic Building Blocks*:* STAMP uses the concept of *commitments* to ensure the privacy of provers. A commitment scheme allows one to commit to a message while keeping it hidden to others, with the ability to reveal the committed value An illustration of STAMP protocol.



VI. CONCLUSION

In this paper,we have presented STAMP,which aims at providing security and privacy to mobile users for their past locations which alredyvisted.we provide a pass key that can be shared to admin .that encrypted key which was generated that can be copied to the checking of an employee/which admin wants.we proposed ,an entropy-based trust model to evaluate the trust level of claims of the past location visitsFrom our experimental results, we observe that under smallkey size settings, our scheme works efficiently in terms of bothcomputational and storage resources. However, the computationallatency could become rather long when large keys aredesired. A major part of computational cost is caused by theBussard-Bagga protocol, which is known for its expensive computationdue to large amount of modular exponentiations [17].Other than defending against the Terrorist Fraud attack (P-Pcollusion), functionalities encounters is specific to the application scenarios) and he/sheintends to make a claim about his/her past STP to the verifier, theSTP claim and verification phase takes place between the prover
and the verifier. A part of the verification job has to be done

Future Enhancement

We introduced the concept of secure location verification and we have shown how it can be used for location based access control, then we presented the STP protocol a simple method for secure location verification.It does not require precise clocks.Hence,we believe that it is suited use in mobile devices.Traditional authentication is based on proving the knowledge of a private key

corresponding to a public key.This protocol prevents frauds where a Certified Authority sits between a legitimate prover and verifier and succeds to perform the distance bounding process. In this paper,only the admin updations,checkings are shown and employee updations,checkings are kept as an open issue.In our paper,we provide a solution of preventing both admin and user by usings three modules.

REFERENCES

[1] S. Saroiu and A. Wolman, "Enabling new mobile applications withlocation 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.

[21] I. Afyouni, C. Ray, and C. Claramunt, "Spatial models for contextaware indoor navigation systems: A survey," *J. Spatial Inf. Sci.*, no. 4, pp. 85–123, 2014.

[22] N. Roy, H. Wang, and R. R. Choudhury, "I am a smartphone and I can tell my user's walking direction," in *Proc. ACM MobiSys*, 2014, pp.