A Survey on Pre LOC Proofs: STAMP

Deepali Alure[1] Prof. Bharati Kale[2]
[1]PG Student [2]Assistant Professor
[1,2]Savitribai Phule Pune University, DPCOE, Wagholi, Pune, India

Abstract— Nowadays location based services are rapidly becoming popular. Many services which are based on user's location can also use the user's location history or their spatial-temporal provenance. It uses GPS technology. Global Positioning System (GPS) is a satellite-based navigation system made up of a network of different satellites. Malicious users may lie about their spatial-temporal provenance without a carefully designed security system for users to prove their past locations. An acronym STAMP stands for Spatial Temporal Provenance Assurance with Mutual Proofs. Basically STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. So it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects user's privacy. A semi-trusted certification Authority is used to distribute cryptographic keys as well as guard users against collusion by light-weight entropy based trust evaluation approach. STAMP is low-cost in terms of computational and storage resources. This protocol is designed to maximize user's anonymity and location privacy. Here users are given the control over the location granularity of their STP proofs. STAMP is collusion resistant. An entropy-based trust model is proposed to detect users mutually generating fake proofs for each other.

Key words: Global Positioning System, Location Proof, Privacy, Spatial-Temporal Provenance

I. INTRODUCTION

Today's many location-based services rely on user's location based on their devices using GPS. It allows some malicious users to fake their STP information. Therefore there is need to achieve integrity of STP proofs. Basically STP stands for Spatial Temporal Provenance where Spatial means something related to space, Temporal means something related to time and last but not the least Provenance is related to history of something.

Most of the existing STP proof schemes rely on wireless infrastructure (e.g. Wi-Fi APs) to create proofs for mobile users. This system proposes 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. However, it may not be feasible for all types of applications, 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.

Following figure shows the system architecture. Basically it works using different devices. There are four types of entities:

1) Prover: A prover is a mobile device which tries to obtain STP proofs at a certain location.
2) 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 are untrusted.

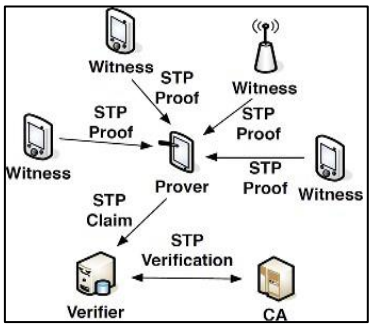

Fig. 1: An illustration of system architecture

3) 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.
4) 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 and trust evaluation.

A prover and a witness communicates with each other via Bluetooth or Wi-Fi in ad hoc mode. The proof generation system of prover is presented a list of available witnesses. When there are multiple witnesses willing to co-operate, 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 connection with CA. Each user can act as a prover or a witness, depending on their roles at the moment. This system assumes 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.

II. LITERATURE SURVEY

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

Author introduces location proofs – a simple mechanism that enables the emergence of mobile applications that require "proof" of a user's location. It allows mobile devices to securely prove their current and past locations. Author presents a concrete protocol which is implementable over Wi-Fi in which APs issue location proofs to mobile devices. A location proof is a piece of data that certifies a geographical location. Access points (APs) embed their geographical location in location proofs, which are then transmitted to designated recipient devices. A location proof has five fields: an issuer, a recipient, a timestamp, a geographical location, and a digital signature. This system describes several potential applications where location

proofs play a central role in enabling them like store discounts for loyal customers, green computing, reducing fraud on auction websites, location-restricted content delivery and police investigations. This system has four security properties like integrity, non-transferability, unforgeability, privacy.

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

This system identified four challenges in designing a location proof architecture and addressed them in VeriPlace. This system illustrated how cryptographic techniques can aid in preserving user privacy and protecting system security. VeriPlace system is a location proof architecture which is designed with privacy protection and collusion resilience. This system 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). Every 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. There are two benefits of this system like user privacy and cheating detection. Author discussed in detail about 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 preserving location proof updating system called APPLAUS. In this system Bluetooth enabled mobile devices mutually generate location proofs and upload to the location proof server. It represents a scheme which relies on both location proofs from wireless APs and witness endorsements from Bluetooth-enabled mobile peers. APPLAUS system can be able to provide real-time location proofs effectively. It preserves source location privacy and it is collusion resistant. Author also developed a user centric location privacy model in which individual users evaluate their location privacy levels in real time and user can decide whether and when to accept a location privacy levels. Betweenness ranking based and correlation clustering-based approaches for outlier detection are also developed here to deal with the colluding attacks,

D. LINK Location verification through immediate neighbors knowledge

For each users location claim, a centralized Location Certifcation Authority (LCA) receives a number of verification messages from neighbors contacted by the claimer using short-range wireless networking such as Bluetooth. The LCA decides whether the claim is authentic or not based on spatio-temporal correlation between the users, trust scores associated with each user, and historical trends of the trust scores. It also detects attacks involving groups of colluding users. Privacy and security analysis : the system also monitor users and requires their credentials to authenticate the proof. In other terms, users are not anonymous regarding the system.

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

Author proposes a scheme which relies on both location proofs from wireless APs and witness endorsements from Bluetooth-enabled mobile peers, so that no users can forge proofs without colluding with both wireless APs and other mobile peers at the same time A secure location-based service requires that a mobile user certifies his position before gaining access to a resource. Currently, most of the existing solutions addressing this issue assume a trusted third party that can vouch for the position claimed by a user. However, as computation and communication capacities become ubiquitous with the large scale adoption of smartphones by individuals, we propose to leverage on these resources to solve this issue in a collaborative and private manner.

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

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 All these location-sensitive applications require users to prove that they really are (or were) at the claimed location. Although 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 proposed system STAMP protocol is represented to provide 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.

Acknowledgement

I would like to take this opportunity to express profound gratitude and deep regard to Prof. Bharati Kale, for her exemplary guidance, valuable feedback and constant encouragement throughout the duration of this work. Her valuable suggestions lift up my work. Her perceptive criticism kept me working to make this research work in much better way. Working under her is an extremely knowledgeable experience for me.

References

[1] Xinlei Wang, Amit Pande, Jindan and Prasant Mohaptra, "STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users,"IEEE Trans. On Networking,Jan 2016.
[2] Saroiu and A. Wolman, "Enabling new mobile applications with location proofs", in Proc. ACM HotMobile, 2009.
[3] W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture", in Proc. ACM GIS, 2010

[4] Z. Zhu and G. Cao, "Towards privacy-preserving and colluding-resistance in location proof updating system", IEEE Trans. Mobile Comput., Jan.2011.
[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.
[7] S. Halevi and S. Micali, Practical and provably-secure commitment schemes from collision-free hashing, in Proc. CRYPTO, 1996.
[8] I. Krontiris, F. Freiling, and T. Dimitriou, Location privacy in urban sensing networks: Research challenges and directions, IEEE Wireless,2010.
[9] Damgrd, Commitment schemes and zero- knowledge protocols, in Proc. Lectures Data Security, 1999.
[10] I. Haitner and O. Reingold, Statistically-hiding commitment from anyone way function, in Proc. ACM Symp. Theory Comput., 2007.

