SPATIAL TEMPORAL PROVENANCE ASSURED WITH MUTUAL PROOF: ENABLING PRIVACY-PRESERVING LOCATION PROOFS FOR MOBILE USERS

[1]Sandeep M N, [2] Dr. K.Thippeswamy

[1]Student, [2] Proffessor and Chairman
[1] Department of Computer Science and Engineering
[1]Visvesvaraya Technological University Department of PG Studies, Regional Office
Mysuru, Karnataka, India

Abstract: **— Location-based services are rapidly becoming extremely 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 (>0.9) collusion detection accuracy.**

***Index Terms*-** **Location proof, privacy, spatial-temporal provenance, trust**

I. 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 may reward 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.

The above applications require users to be able to obtain proofs from the locations they visit. Users may then choose to present one or more of their proofs to a third-party verifier to claim their presence at a location at a particular time. In this paper, we define the past locations of a mobile user at a sequence of time points as the *spatial-temporal provenance* (STP) of the user, and a digital proof of user's presence at a location at a particular time as an *STP proof*. Many works [1]–[3] in literation have referred to such a proof as *location proof* . 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 temporal information. Other terminologies have been also used for similar concepts, such as location claim [4], provenance proof [5], and location alibi [6].

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 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. 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 A who is at an intended location masquerades as another colluding user and obtains STP proofs for B. 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 [8] 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.

The *contributions* of this paper can be summarized as:

1) A distributed STP proof generation and verification protocol (STAMP) is introduced to achieve integrity and non transferability of STP proofs. No additional trusted third parties are required except for a semi-trusted CA.

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

3) STAMP is collusion-resistant. The Bussard-Bagga distance bounding protocol [9] 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 to STAMP to facilitate the utilization of stationary wireless 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(5%) of colluding attackers.

II. Related work

The notion of unforgeable location proofs was discussed by Waters *et al.* [9]. 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.

Hasan et al. [5] proposed 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. It eliminates the necessity of multiple trusted parties. Two privacy preserving schemes based on hash chains and Bloom filters respectively are described for protecting the integrity of the chronological order of location proofs. 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 design a framework that can also work for distributed scenario where users are far from any trusted AP.

In Davis *et al.*'s ***alibi system*** [6], their private corroborator scheme relies on mobile users within proximity to create alibi's(i.e., location proofs) for each other. The security and privacy of the system is achieved based on a cryptographic commitment scheme. However, they do not deal with any collusion attacks. Also, multi-level location granularity is not considered in their work.

The system that is most closely related to our work is Zhu *et al.*'s ***APPLAUS*** [3]. It is a location proof system that is also based on co-located mobile devices mutually generating location proofs. 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 redundant for accomplishing the goals. Periodically changed pseudonyms incur high operational overhead because of the requirement for highly cautious management and scheduling. Dummy proofs have to be regularly generated in order to achieve the privacy properties, which also incur high communication and storage overhead. The collusion detection in APPLAUS is based on betweenness ranking and correlation clustering. These approaches require the location proof server to have access to at least the majority of the concurrent (within a short delay)location proofs at the same location (within a small region).This needs users to submit their location proofs right after generating them, which is infeasible when there is no Internet connection on-the-spot. Moreover, these approaches cost large computing power to run the detection (>200 seconds for 5000 pseudonyms) and their successful detection ratio is high (>0.9) only when the percentage of the colluding attackers is rather low.

III. SYSTEM MODEL

The 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 of applications.

Fig. 1 illustrates the architecture of our system. There are four types 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 in proximity with the prover and is willing to create an STP proof for the prover upon receiving his/her request.

- **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 which issues, manages cryptographic credentials for the other parties. CA is also responsible for proof verification and trust evaluation.

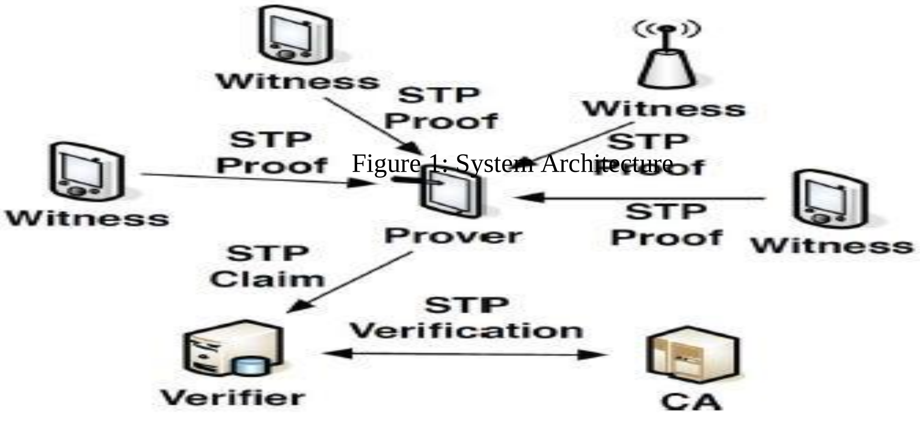

Figure 1: System Architecture

Fig: 1. An illustration of System Architecture

A prover and a witness communicates with each other via Bluetooth or WiFi in ad hoc mode.. The proof generation system of prover is presented a list of available witnesses. 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.

IV. RESULTS DISCUSSION

This protocol uses SHA-1 algorithm which ensures secured communication between a honest prover and a honest verifier. The employee in an organization can prove his location without any fraud. The fraud is prevented by encrypting and then decrypting the location proofs.

V. CONCLUSION AND FURTHER ENHANCEMENT

In this paper the protocol deals with the honest communication between a prover and a verifier. The employee can prove his location using Certificate Authority through verifier. The verifier cannot fraud the location proofs of prover and the witness because of encryption done by the prover and verifier. Hence no frauds can be done. In future we can have a mobile application for it, where it can be implemented in actual organizations and see the results.

VI. ACKNOWLEDGEMENT

I would like to thank Dr K Thippeswamy Professor and Chairman, Department of Studies in Computer Science and Engineering, V.T.U Regional Office, Mysuru and Anonymous reviewers encouragement and constructive piece of advice that have prompted us for new round of rethinking of our research and additional experiment and clearer presentation of technical content.

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 WirelessCommun.*, vol. 17, no. 5, pp. 30–35, Oct. 2010.
[8] L. Bussard and W. Bagga, "Distance-bounding proof of knowledge to avoid real-time attacks," in *Security and Privacy in the Age of UbiquitousComputing*. New York, NY, USA: Springer, 2005.
[9] X. Wang *et al.*, "STAMP: Ad hoc spatial-temporal provenance assurance for mobile users," in *Proc. IEEE ICNP*, 2013, pp. 1–10.