International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com
ISSN No: 2456 - 6470 | Volume - 2 | Issue – 6 | Sep – Oct 2018

Supporting Spatial-Temporal Provenance Location Proofs for Ad-Hoc Mobile Users

K. Dhanalakshmi
Lecturer Sr. Grade, Department of Computer Engineering,
Ayya Nadar Janaki Ammal Polytechnic College, Sivakasi, Tamilnadu, India

ABSTRACT

Spatial-Temporal Provence (STP) are quickly becoming immensely popular. In apply the position that users of the communicate to the location-based services (LBS). Malicious users may lie about their spatial-temporal provenance (STP) without a carefully designed security system for users to prove their past locations. This type of attack will have a severe impact on applications of the period of time traffic office, location based on the access management, the traffic of the process to be in electronic election. 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, LP versions 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 collusion detection accuracy.

Keyword: *spatial-temporal provenance, location proof and STAMP*

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. 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 centre 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 in liberation 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, provenance proof, and location alibi.

II. SYSTEM MODELING

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.

Hasanet al. 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.

In Davis et al.'s alibi system, their private corroborator scheme relies on mobile users within proximity to create alibi's (i.e., location proofs) for each other.

As we explained, 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 of applications. We design a generic decentralized protocol, and then show how it can work well for centralized case also.

Fig.1 An illustration of system architecture

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. The witness can be untrusted or trusted, and the trusted witness can be mobile or stationary (wireless APs). Collocated mobile users are untrusted.
- Verifier: A verifieris 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 and trust evaluation.

A prover and a witness communicate with each other via Bluetooth or WiFi in ad hoc mode. A peer discovery mechanism for discovering nearby witness is required and preferably provided by underlying communication technology instead of our protocol. The proof generation system of prover is presented a list 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 connection with 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. There are strong incentives for people not to give their privacy away completely, even to their families or friends, so we assume a user never gives his/her mobile device or private key to another party.

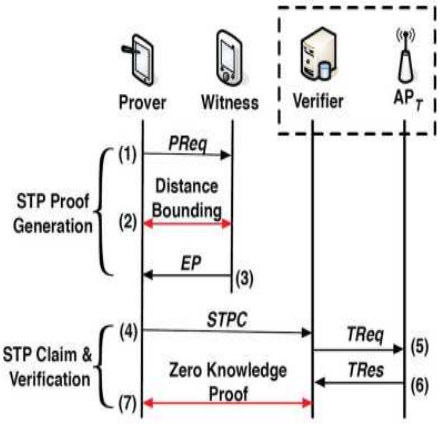

Fig.2 STAMP protocol with trusted wireless AP

III. SECURITY ANALYSIS

In this section, we analyze the security properties of the STAMP protocol and prove that the protocol can achieve our security goals.

Proposition 1: A prover cannot create a legitimate without a witness.

Proposition 2: Without colluding with a witness, a prover cannot create a legitimate *EP* without being present at the claimed location at the claimed time

Proposition 3: A prover cannot change the spatial and/or temporal information in an *EP*

Proposition 4: A prover cannot use an *EP* created for another prover.

Proposition 5: A witness cannot repudiate a legitimate *EP* created by him/her

Proposition 6: A prover and a witness cannot find out each other's identity.

Proposition 7: P Reqs sent from the same prover for different STP proof collection events are unlikable to a witness.

Proposition 8: STP proofs generated from the same witness for different STP proof collection events are unlikable to a prover

Proposition 9: The lowest location level a verifier learns about a prover is the level that the prover intends to reveal to him/her.

Proposition 10: CA cannot learn any location information about a prover or witness from V Req.

Proposition 11: Trusted users increase the overall trust of the system.

Proposition 12: Nobody can fake himself/herself as a trusted user.

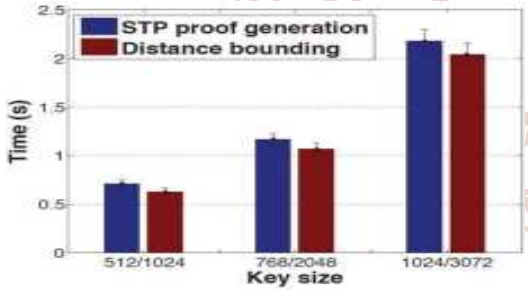

Fig.3 Time to generate an STP proof under different key sizes

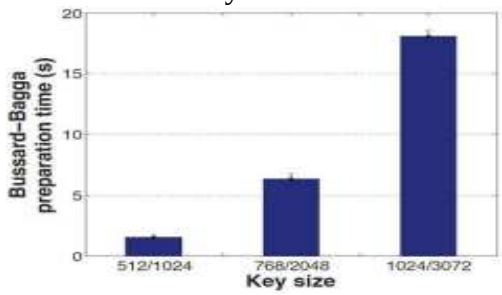

Fig.4 Time of Bussard-Bagga preparation stage under different key sizes

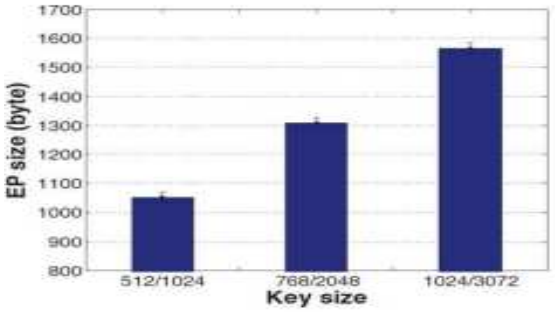

Fig.5 Size of EP under different key sizes

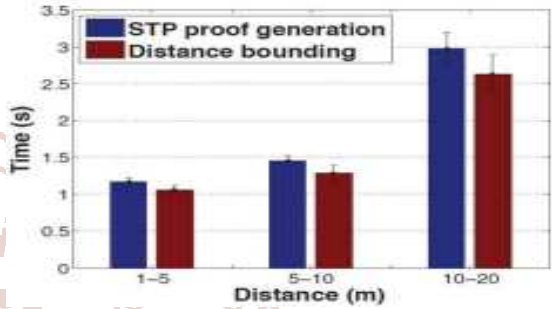

Fig.6 Time to generate an STP proof under different communication distances

We implemented a prototype client application on Android with Java. Our experiments are carried out on two Samsung Exhibit II 4G devices equipped with Qualcomm MSM 8255 1 GHz chipset, 512 MB RAM, 1 GB ROM, GPS, and Bluetooth, and running Android OS 2.3. Bluetooth is used as the communication interface between mobile devices. We use DSA key pairs for signing/authentication operations because DSA is based on the discrete-log problem, which makes it possess the mathematical properties desired by the Bussard-Bagga protocol. Since DSA is not designed for encryption/decryption purpose, we use RSA key pairs as sub-keys for encryption/decryption operations

.

IV. RESULTS AND DISCUSSIONS

From our experimental results, we observe that under small key size settings, our scheme works efficiently in terms of both computational and storage resources. However, the computational latency could become rather long when large keys are desired. A major part of computational cost is caused by the Bussard-Bagga protocol, which is known for its expensive computation due to large amount of modular exponentiations. Other than defending against the Terrorist Fraud attack (P-P collusion), functionalities of STAMP do not specifically rely on the Bussard-Bagga protocol. Therefore, under circumstances where P-P collusion is not a concern, we suggest to disable the Bussard-Bagga stages in STAMP, which

will result less than 0.2 s for each STP proof transaction (distance bounding time deducted from STP proof generation time) without the necessity of the preparation stage. Furthermore, active on-going research in the location verification field is being conducted to achieve the same security property as the Bussard-Bagga protocol with much better performance. A new distance bounding scheme can be easily plugged into STAMP and replace the Bussard-Bagga protocol. It is also a part of our future work to investigate such possibilities.

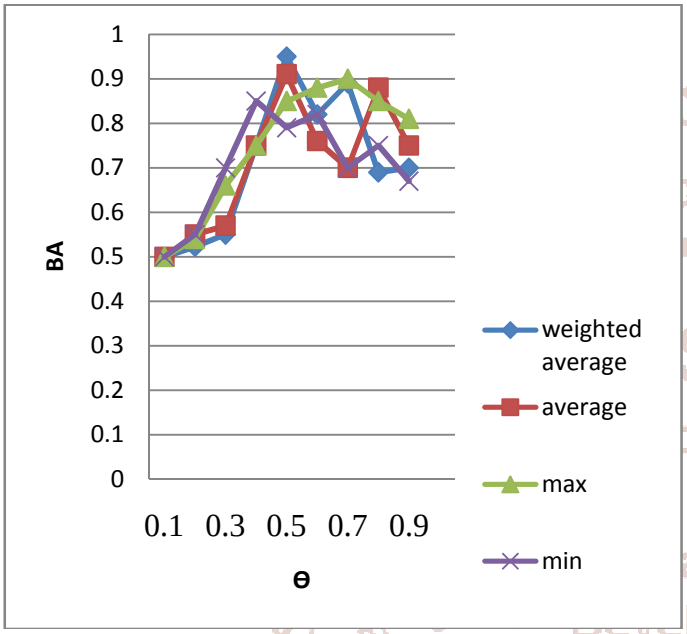

Fig.7 BA under different trust consolidation functions

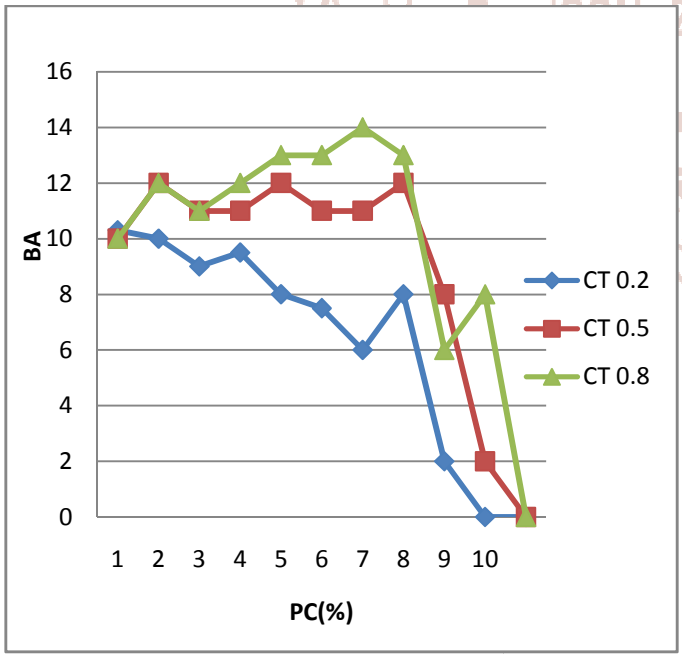

Fig.8 BA under different percentage of Colluding attackers and collusion tendency

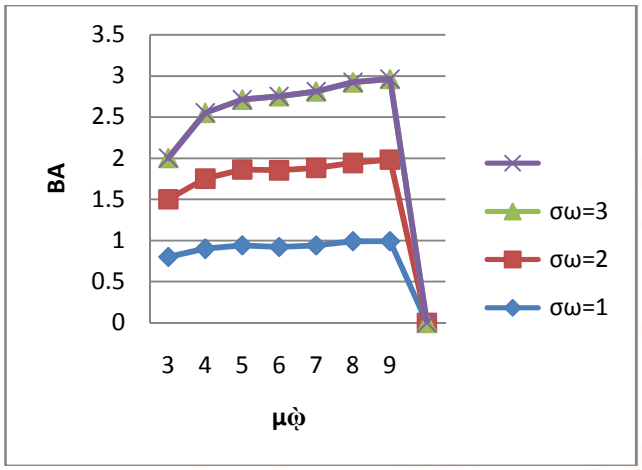

Fig.9 BA under different number of witnesses

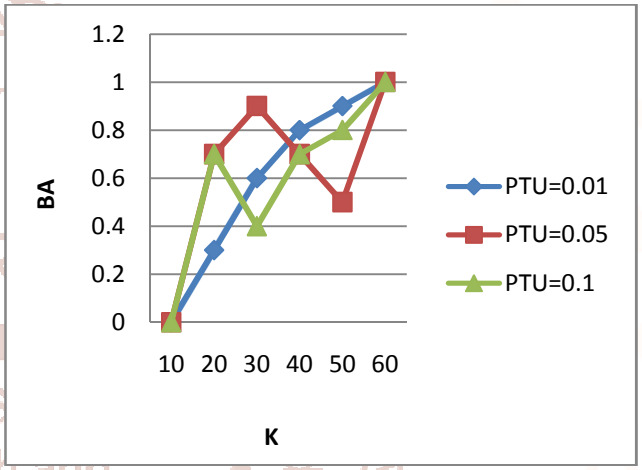

Fig.10 BA under different k and percentage of trusted users

Bluetooth is a ubiquitous short-range, low-power communication technology that also provides a robust device discovery mechanism, making it a logical choice for implementing our prototype. As observed in evaluation, limited range and discovery latency due to underlying Bluetooth technology exerts another negative impact on performance of our protocol, especially in high mobility scenarios. Such drawbacks are not unique for our scheme and several methods, have been proposed to achieve a trade-off between discovery and latency which we can adapt in our future work. Furthermore it is necessary to emphasize that our protocol for proof generation is designed to be agnostic of communication technologies and should be interoperable with other types of ad hoc connections such as Wi-Fi mesh and vehicle networks. Appropriate method can be selected adaptively according to different situations with respect to mobility, witness density, etc. We intend to implement a framework in our future prototype to facilitate the switch among multiple compatible communication methods.

Our P-W collusion detection is supported by entropy-based trust evaluation, instead of complex graph algorithms like the ones used by the APPLAUS system. Therefore, each run of our P-W collusion detection only requires a number of cheap computations. It is much more efficient than APPLAUS where a few hundred seconds are needed to run detection among a few thousands of users. The weakness of our detection, however, is that if attackers only launch collusions very infrequently, or if there is a large pool of users that an attacker can choose to collude with, the accuracy may drop significantly. Nevertheless, unless trusted infrastructures are deployed at every location, it is always hard to tell if an STP proof is a result of collusion or not. Our trust model serves as a good countermeasure so that malicious users are deterred from launching collusions of their own free will or with only a small group of users. In many cases, people are around with their family members and friends more often; this will inevitably affect people's entropy. However, we consider this as a general case for most of the users and thus it is possible to adjust the parameter in to maintain an un shifted trust range. We leave the investigation of how exactly such a social pattern affects our trust evaluation as future work.

V. CONCLUSION

STAMP relies on mobile devices in vicinity to mutually generate location proofs or uses wireless Aps to generate location proofs which aims at providing security and privacy assurance to mobile users' proofs for their past location visits. Integrity and non-transferability of location proofs and location privacy of users are the main design goals of STAMP. Two collusion scenarios are specified namely: P-P collusion and P-W collusion. To protect against P-P collusions, we integrated the Bussard-Bagga distance bounding protocol into the design of STAMP. To detect P-W collusion, we proposed an entropy-based trust model to evaluate the trust level of claims of the past location visits. Our security analysis shows that STAMP achieves the security and privacy objectives. Our implementation on Android smart phones indicates that low computational and storage resources are required to execute STAMP. STP posted data is further encrypted using a symmetric key known only between the user and the service provider.

VI. REFERENCES

1. S. Saroiu and A. Wolman, “Enabling new mobile applications with location proofs,” in Proc. ACM Hot Mobile, 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,” CoRR2011.
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, un observability, and pseudonymity-a proposal for terminology,” in Designing Privacy Enhancing Technologies. New York, NY, USA: Springer, 2001.
13. Y.-C. Hu, A. Per rig, and D. B. Johnson, “Wormhole attacks in wireless networks,” IEEE J. Sel. Areas Common., vol. 24, no. 2, pp. 370–380, Feb. 2006