International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Accredit Isolation Preserving where about Certification for Mobile Users

E. Ravindera Reddy*1, Singampalli Sankeerthi2

*1Assistant Professor, Department of CSE, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India
2 M.TECH Student, Department of CSE, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

Location-based services are quickly becoming immensely 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 lightweight 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.

Keywords: Spatial-Temporal Provenance, Location Proof, Privacy, 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 literati on 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 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 literati on 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 no 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 B and obtains STP proofs for 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 Terorist 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 [9] 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 an entropy-based trust model to guard users from proper-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 high percentage (_5percentage) of colluding attackers.

II. RELETED WORK

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.

DISADVANTAGES OF EXISTING SYSTEM:

- 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.
- Most of the existing schemes require multiple trusted or semi-trusted third parties.

III. PROPOSED SYSTEM:

- 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.
- 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.
- We propose an entropy-based trust model to detect the collusion scenario.

- 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.
- STAMP is designed to maximize users' anonymity and location privacy. Users are given the control over the location granularity of their STP proofs.
- 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.
- STAMP uses an entropy-based trust model to guard users from proper-witness collusion. This model also encourages witnesses against selfish behavior.

ADVANTAGES OF PROPOSED SYSTEM:

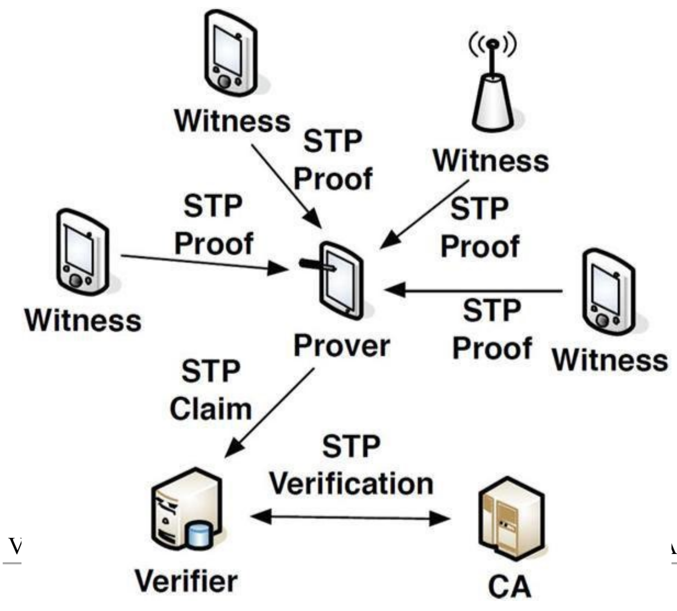
- Target a wider range of applications.
- STAMP is based on a distributed architecture.
- STAMP requires only a single semi-trusted third party, which can be embedded in a Certificate Authority (CA).

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).

STAMP requires low computational overhead.A security analysis is presented to prove STAMP achieves the security and privacy objectives.

SYSTEM ARCHITECTURE:



MODULES:

- Prover
- Witness
- Verifier
- Certificate Authority (CA)

MODULES DESCRIPTION:

Prover:

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 should also be preserved. Since a witness who agrees to create an STP proof is co-located with the proper, his/her identity should not be revealed to the prover. Prover needs to reveal both his/her identities and STP information in order to get services from a verifier, the proper does not necessarily trust the verifier completely. When approver tries to claim his/her location at a particular time to a verifier, he/she should not be obligated to reveal his/her most accurate location to the verifier.

Witness:

A witness is a device, which is in proximity with the proper and is willing to create an STP proof for the proper 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 witness who receives a decides if he/she accepts the request. If the request is accepted, the witness sends a back to the proper, after which, the two party's start the execution of the distance bounding stage of the Bussard-Bagga protocol. This enables the witness to know that the party who is requesting an STP proof is within a certain range. However, the witness has no way to verify if the party has the private key, which in fact corresponds to the committed identity. The witness cannot carry out the zero-knowledge proof stage because it requires the knowledge of the prover's public key.

Verifier:

Verifier: A verifier is the party that the proper wants to show one or more STP proofs to and claim his/her presence at a location at a particular time. When a proper encounters a verifier, (the frequency of such encounters is specific to the application scenarios) and he/she intends to make a claim about his/her past STP to the verifier, the STP claim and verification phase takes place between the proper and the verifier. A part of the verification job has to be done by CA. Therefore, communication between the verifier and CA.

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. Each user can act as a provider or a witness, depending on their roles now. 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.

IV. IMPLEMENTATION

MODULES:

- Prover
- Witness
- Verifier
- Certificate Authority (CA)

MODULES DESCRIPTION:

Prover:

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 should also be preserved. Since a witness who agrees to create an STP proof is co-located with the provider, his/her identity should not be revealed to the prover. Prover needs to reveal both his/her identities and STP information in order to get services from a verifier; the provider does not necessarily trust the verifier completely. When approver tries to claim his/her location at a particular time to a verifier, him /her

IMPLEMENTATION MODULES:

Prover
Witness
Verifier
Certificate Authority (CA)

MODULES DESCRIPTION:

Prover:

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 should also be preserved. Since a witness who agrees to create an STP proof is co-located with the prover, his/her identity should not be revealed to the prover. Prover needs to reveal both his/her identities and STP information in order to get services from a verifier; the prover does not necessarily trust the verifier completely. When approver tries to claim his/her location at a particular time to a verifier, him /her

Be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

When the data is entered, it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN:

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system, results of processing are communicated to the users and to other system through outputs. In output design, it is determined how the information is to be displaced for immediate need and the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

Convey information about past activities, status or projections of the Future.
Signal important events, opportunities, problems, or warnings.

Trigger an action.
Confirm an action.

V. CONCLUSION

In this paper, we have presented STAMP, which aims at providing 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. We have specifically dealt with two collusion scenarios: 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. Extensive simulation results show that our trust model is able to attain a high balanced accuracy with appropriate choices of system parameters.

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,"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 context aware 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. 329-342.

[23]. R. Steinbach, J. Green, and P. Edwards, "Look who's walking: Social and environmental correlates of children's walking in London," Health Place, vol. 18, no. 4, pp. 917-927, 2012.

[24]. K. Brodersen, C. Ong, K. Stephan, and J. Buhmann, "The balanced accuracy and its posterior distribution," in Proc. IEEE ICPR, 2010, pp. 3121-3124.

[25]. B. Peterson, R. Baldwin, and J. Kharoufeh, "Bluetooth inquiry time characterization and selection," IEEE Trans. Mobile Comput., vol. 5, no. 9, pp. 1173-1187, Sep. 2006.

[26]. J. Zhu, K. Zeng, K.-H. Kim, and P. Mohapatra, "Improving crowdsourced Wi-Fi localization systems using Bluetooth beacons," in Proc. 9th Annu. IEEE SECON, Jun. 2012, pp. 290-298.