Privacy Ensured Location Proof Updates for Mobile Applications

Sarlana Sandhya Rani[1], Apurva Khandekar[2]

[1,2]*Associate Professor, Department of Computer Science and Engineering*
[1,2]*Malla Reddy Engineering College (A), Maisammaguda, Hyderabad, Telangana, India.*

Abstract

Today location-sensitive service relies on user's mobile device to determine its location and send the location to the application. A Privacy-Preserving Loc Ation proof Updating System (APPLAUS). Recent advances in sensing, computing, and networking have paved the way for the emerging paradigm of Mobile Crowd Sensing (MCS). The openness of such systems and the richness of data MCS users are expected to contribute to them raise significant concerns for their security. We propose to leverage on these resources to solve this issue in a collaborative and private manner. The system consists of Server and client. Server contains sensitive files, clients always trying to download these files from server. Prover application which will key monitor client location details and send these details in periodical intervals of time to the verifier service in server We formally assess the achieved security and privacy properties our system offers strong security and privacy-preservation guarantees facilitating the deployment of trustworthy MCS applications. APPLAUS can be implemented with the existing network infrastructure and the current mobile device is easily deployed in Bluetooth enabled mobile devices with little computation or power cost. Extensive experimental results show that our algorithms besides providing location proofs effectively and significantly preserve the source location privacy.

Index Terms: *Mobile Crowd Sensing, Security, Privacy, Incentive Mechanisms, location proof, location privacy, pseudonym.*

1. Introduction

Mobile devices, such as smart phones and PDAs, are playing an increasingly important role in people's lives. Location based services take advantage of user location information and provide mobile users with a unique style of resource and services [1]. Nowadays more and more location-based applications and services require users to prove their locations at a time. We propose A Privacy-Preserving LocAtion proof Updating System (APPLAUS), which does not rely on the wide deployment of network infrastructure or the expensive trusted computing module [2]. In APPLAUS, Bluetooth enabled mobile devices in range mutually generate location proofs, which are uploaded to a untrusted location proof server that can verify the trustworthy level of each location proof. An authorized verifier can query and retrieve location proofs from the server [3]. Mobile Crowdsensing [4] (MCS) has emerged as a novel paradigm for data collection and collective knowledge formation practically about anything, from anywhere and at any time.

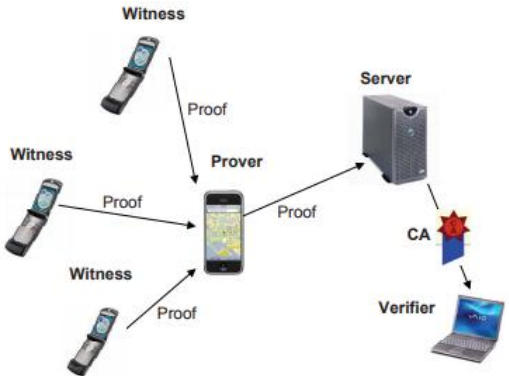

Figure 1. Location Proof Updating and Message Flow

This new trend leverages the proliferation of modern sensing capable devices in order to offer a better understanding of people's activities and surroundings. Emerging applications range from environmental monitoring [5] to intelligent transportation [6] and assistive healthcare [7]. MCS users are expected to contribute sensed data tagged with spatio-temporal information which, if misused could reveal sensitive user-specific information such as their whereabouts and their health condition [8]. Even worse, data contributions are strongly correlated with the current user context there is a significant risk of indirectly inferring daily routines or habits of users participating in MCS applications.

2. Related Work

Recently several systems have been proposed to give end users the ability to prove that they were in a place at a time [9]. Relies on the fact that nothing is faster than the speed of light in order to compute an upper bound of a user distance [10]. Proposes challenge-response schemes, which use multiple receivers to accurately estimate a wireless node location using RF propagation characteristics the authors propose a privacy-preserving data reporting mechanism for MCS applications. The intuition behind this work is that user privacy is protected by breaking the link between the data and the participants. Nonetheless, opposite to our work, the proposed scheme solely focuses on privacy and, thus, does not consider incentive mechanisms and accountability for misbehaving users [11]. Addressing aspects beyond the scope of this work the authors propose a reputation-based mechanism for assessing the data-trustworthiness of user contributed data leverages machine learning techniques to detect and sift faulty data originating from adversarial users seeking to pollute the data collection process [12]. Recently, Wang and co-authors propose STAMP [13]. In the same spirit as PROPS, a proverb convinces a verifier of his location by showing several LPSs. STAMP ensures the authenticity of LPS the no transferability and the anonymity of prover and witnesses generating the proof. Users have also the possibility to choose the granularity to reveal to a verifier in contrast to PROPS, the LPSs are encrypted under the CA public key, thus the prover cannot check himself the validity of location information endorsed by the witness [14]. Geo-location data is gathered in several ways, including built-in Global Positioning System devices, IP address, or Wi-Fi network mapping. Location proof plays a vital role in location sensitive applications. Location sensitive applications such as Location based access [15].

3. System Model

Organizations or individuals initiating data collection campaigns by recruiting users and distributing sensing tasks to them The TI initiates sensing tasks and campaigns. Each task is essentially a specification of the sensor's users must employ, the area of interest, and the lifetime of the task. Operators of sensing capable mobile devices and navigation modules Devices possess transceivers allowing them to communicate over wireless local area [16]. System entities responsible for supporting the lifecycle of sensing tasks: they register and authenticate users, collect and aggregate user-contributed reports and, finally, disseminate the results to all interested stakeholders. MCS can be abused both by external and internal adversaries. The former are entities without any established association with the system their disruptive capabilities are limited. They might also manipulate the data collection process by contributing unauthorized samples or replaying the ones of benign users [17]. The MCS application such adversaries, can submit faulty yet authenticated, reports during the data collection process. Their aim is to distort the system's perception of the sensed phenomenon, and thus, degrade the usefulness of the sensing task [18].

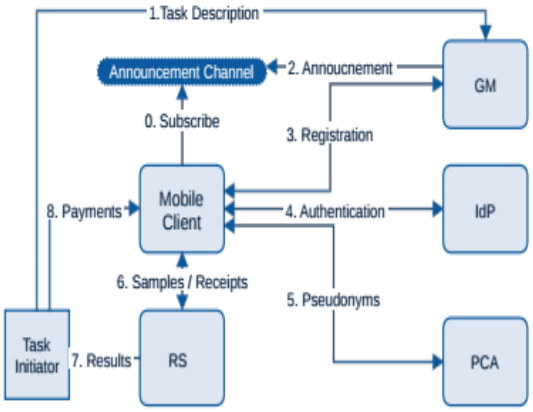

Figure 2. System Overview

4. Proposed System

Aim of proposed system is to design architecture of system, such that it needs to provide secure and efficient access to system without compromising the security, privacy of user and preventing un-authorized to access the system to perform this functions [19], Location information is identified by using geographical representations through latitude and longitude points. We implement an Advanced System for Location Tracking and Updating in which co-located Wi-Fi enabled mobile devices mutually generate location proofs and update to a location proof server. By this it is easy to find the exact location of the client using a web portal, accessed by a Server by simply login into the system [20]. The users must register with the CA (certificate authority). CA will generate credentials in the form of pseudonyms. These credentials send to the user mail ID by CA. Using these credentials user can able to login to the system and they can access the system, if user prove that they are at claimed location and they are trusted [21].

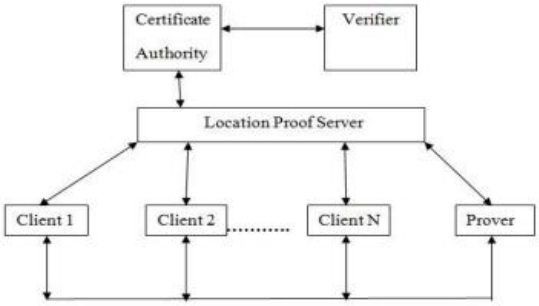

Figure 3. Proposed system Architecture

4.1. Source Location Privacy

Now we look at how an adversary may reveal location information by analyzing the location proof history. Suppose the attacker has sufficient resources the attacker may simply monitor and examine the content of a record that may contain the user's identity and location even if the user's ID is encrypted or pseudonym zed, it is easy for the adversary to trace back all the location activities related to the same ID once its pseudonym is discovered. According to [22], a mechanism to achieve anonymity appropriately combined with dummy traffic yields unobservability which is the state that Items of Interests (IOIs) are indistinguishable from any IOI of the same type. All the subjects and events under consideration constitute an unobservability set.

Algorithm

Input: time t of incoming location proof exchange request;

1: calculate location privacy loss Δ when assuming the incoming request is accepted.

2: if $\Delta > \epsilon$, ϵ is pre-defined location privacy loss threshold then.

3: deny location proof exchange request

4: else

5: accept location proof exchange request

6: end if

4.2. Hash Chains

As mentioned previously, the user of a location proof system should have the possibility to reveal different granularities of the positions contained in the LPSs he collected, and coauthors propose to solve this problem by the use of multiple encryption. More precisely when creating an LPS, each witness generates five different granularities of the location of the prover [23]. The granularities are then encrypted with different keys using a symmetric encryption algorithm such as AES. The encrypted values are then endorsed by the witness and put in the LPS. When a prover reveals his location up to a granularity to a verifier, he simply sends the decryption key corresponding to the granularity he wishes to disclose [24].

Algorithm: Verification of Location Proof

Decrypt the content sent by the user /witness using server's private key, now Verifier has following data and it verifies.

Twitt=Time of witness, L=Location, Pwitt= Pseudonym of witness, Switt= Signature of witness, H(M)=Hash function of M.

Create a M using following formula and using HASH function create H(M)|

M=Pprov || Rprov || Twitt || L

1. H(M) and H(M)' are equal proceed else message is hacked in middle.
2. Verify Twitt from Witness message with Time validity when the Location Proof was conducted from sever table. If fails return Time Expired message.
3. Verify Pwitt from Witness message with DB. If fails return Pseudonym fails message.
4. Verify with Pprov get from encrypted message with Pprov given by Prover. If fails return Pprov fails.
5. Verify with Rprov get from encrypted message with Rprov given by Prover. If fails return Rprov fails.
6. Verify with Location (L) get from encrypted message with Location (L) given by Prover. If fails return Location fails.

If all these six conditions are passed, make the status of Witness in Server table as trusted else make it as un-trusted and mention the condition.

5. Performance Evaluation

In this section, we consider deployment feasibility for APPLAUS, including the computation and storage constraint, power consumption, as well as the proof exchange latency. We also use simulations to compare the performance of APPLAUS with a baseline scheme, and evaluate the privacy level against powerful statistical analysis attacks. We also measure the performance with two metrics: proof exchange time latency and power consumption.

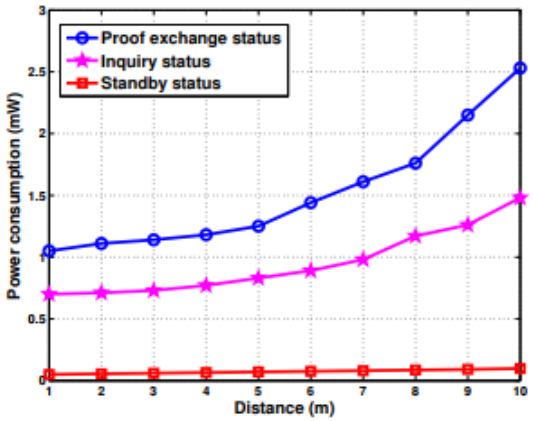

Figure 4. Performance of power consumption

During our evaluation, we use three metrics: message overhead ratio, proof delivery ratio, and average delay. The message overhead ratio is defined as the ratio of dummy traffic and real proof traffic. The proof delivery ratio is the percentage of location proof message that is successfully uploaded to the location proof server.

6. Conclusions

This paper proposed a privacy-preserving location proof updating system, called APPLAUS, in which co-located Bluetooth enabled mobile devices mutually generate location proofs, and upload to the location proof server. We use statistically changed pseudonyms for each device to protect source location privacy from each other, and from the untrusted location proof server. we presented a novel secure and accountable MCS architecture that can safeguard user privacy while supporting user incentive mechanisms. Our architecture achieves security, privacy and resilience in the presence of strong adversaries.

For more security reasons not only IP address, MAC address is also included in this system for verification. This will be help full in secure location-based file accessing system. Finally, another research avenue is the design of a secure multiparty computation version of the protocol involving a joint interaction with the prover and multiple witnesses rather than relying on pairwise interactions between the prover and each witness

References

[1] S. Saroiu and A. Wolman, “Enabling new mobile applications with location proofs,” in Proc. ACM HotMobile, 2009, Art. no. 3.

[2] S. Brands and D. Chaum. Distance-bounding protocols. In Advances in Cryptology-EUROCRYPT, 1994.

[3] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In IEEE INFOCOM, 2005.

[4] S. Gisdakis et al. “Secure & Privacy-Preserving SmartphoneBased Traffic Information Systems”. In: IEEE Transactions on ITS (2015), pp. 1428–1438.

[5] A. Thiagarajan et al. “VTrack: Accurate, Energy-aware Road Traffic Delay Estimation Using Mobile Phones”. In: Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems. Berkeley, USA, 2009.

[6] S. Gisdakis et al. “SEROSA: SERvice oriented security architecture for Vehicular Communications”. In: IEEE Vehicular Netw Conf. Boston, USA, 2013, pp. 111–118.

[7] T. Giannetsos, T. Dimitriou, and N. R. Prasad. “Peoplecentric sensing in assistive healthcare: Privacy challenges and directions”. In: Security and Communications Network 4.11 (Nov. 2011), pp. 1295–1307.

[8] D. Christin et al. “A Survey on Privacy in Mobile Participatory Sensing Applications”. In: J. Syst. Softw. 84.11 (2011), pp. 1928–1946.

[9] K. Fall. A delay-tolerant network architecture for challenged internets. In ACM SIGCOMM, 2003.

[10] W. Gao and G. Cao. Fine-grained mobility characterization: steady and transient state behaviors. ACM, 2010.

[11] Xinlei Oscar Wang et al. "ARTSense: Anonymous reputation and trust in participatory sensing." In: 32nd Int. Conference on Computer Communications. Turin, Italy, 2013.

[12] S. Gisdakis, T. Giannetsos, and P. Papadimitratos. "SHIELD: A Data Verification Framework for Participatory Sensing Systems". In: ACM Conference on Security & Privacy in Wireless and Mobile Networks. New York, 2015.

[13] X. O. Wang, J. Zhu, A. Pande, A. Raghuramu, P. Mohapatra, T. Abdelzaher, and R. Ganti. Stamp: Ad hoc spatial-temporal provenance assurance for mobile users.

[14] B. Waters and E. Felten. Secure, private proofs of location. Technical report, Department of Computer Science, Princeton University, Tech. Rep. TR-667-03, 2003.

[15]. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-Based Trust for Mobile User-Generated Content:applications Challenges and Implementations," Proc. Ninth Workshop Mobile Computing Systems and Applications, 2008.

[16] Xinglin Zhang et al. "Free Market of Crowdsourcing: Incentive Mechanism Design for Mobile Sensing". In: IEEE Trans. Parallel Distrib. 25.12 (2014), pp. 3190–3200.

[17] I. Koutsopoulos. "Optimal incentive-driven design of participatory sensing systems". In: INFOCOM, 2013 Proceedings IEEE. 2013, pp. 1402–1410.

[18] Long Pham et al. "Multi-attribute online reverse auctions: Recent research trends". In: European Journal of Operational Research 242.1 (2015), pp. 1–9.

[19]. S.Saroiu and A. Wolman, "Enabling New Mobile Applications with Location Proofs," Proc. ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile '09), 2009.

[20]. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-Based Trust for Mobile User-Generated Content:applications Challenges and Implementations," Proc. Ninth Workshop Mobile Computing Systems and Applications, 2008.

[21]. W. Luo and U. Hengartner. Proving your location without giving up your privacy. In ACM HotMobile, 2010.

[22] I. Rhee, M. Shin, K. Lee, and S. Chong. On the Levy-walk Nature of Human Mobility. In IEEE INFOCOM, 2007.

[23] C.-P. Schnorr. Efficient identification and signatures for smart cards. In Advances in Cryptology, 1990.

[24] M. Talasila, R. Curtmola, and C. Borcea. Link: Location verification through immediate neighbors knowledge. Springer, LNICST 73, 2012.