Authorized Updation of Ensured Location in Geosocial Applications

Thangalla Palli Sahithi[1], Margani Harinadha[2]

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

Abstract

Here, LocX, a novel alternative that provides significantly improved location privacy without adding uncertainty into query results or relying on strong assumptions about server security is presented. We use cloud storage controlled by users themselves as storage facilities and they do not need to worry about any untrusted third party. We implement Android Cloud Tracker prototype on Android phones, and the evaluation shows that it is both practical and lightweight it generates a small amount of data flow and its distributed architecture provides strong guarantees of location privacy while preserving the ability to efficiently track missing devices. Our protocol exploits unique Wi-Fi signal characteristics and employs an information theoretically secure fuzzy vault scheme. Our solution is faster by an order of magnitude and the performance of our scheme is independent of the location tag size and distance between the mobile user and location proof provider compared to the state-of-the-art. This is mainly based on the model like the block chain model in Bitcoin with a global consistency check ensure entity is being dishonest about the location information. We have used the EigenTrust and Peer Trust check methodologies to calculate global and personalized trust matrix while confirming attestation.

***Index terms**: Location privacy, security, location-based social applications, location transformation, efficiency, Wireless channel characteristics, Fuzzy vault.*

1. Introduction

The mobile devices have led to the rapid increase in various location-based applications and services [1]. Location based applications such as foursquare award incentives to mobile users who check-in most frequently at a location. Additionally, the owner of the location also rewards mobile user with gift vouchers [2]. These location-based applications/services (LBS) can be further applied to other access control systems where proximity detection is required [3]. A Location-Based Service (LBS) takes advantage of the position of its users to deliver a service tailored to their current or past geo located context. In practice the position that a user transmits to an LBS is often computed determined by his own device. Thus, a malicious user can lie about his position by having his device transmitting a location of his choice [4]. This type of attack can have a severe impact on applications such as real-time traffic monitoring, location-based access control, discount tied to the visit of a shop or local electronic election, to name a few [5].

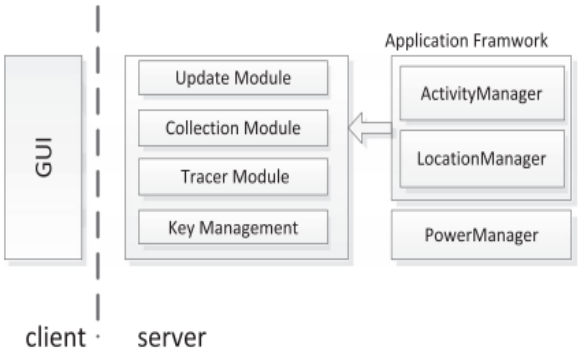

Figure 1. Modularized Android Cloud

A traditional standard device tracking system consists of a client hardware or software logic installed on the device related cryptographic key material stored on the device or maintained separately by the owner and a remote storage facility [6]. The client sends location updates to the remote storage over the Internet. Once the device goes missing, the owner searches the remote storage for location updates pertaining to the device's current whereabouts [7].

2. Related Work

The location proofs as a new mechanism that enables the existence of mobile applications that needs proof of the user's location [8]. It is handled by the wireless access point to mobile devices. The solution is mainly based on users and wireless access points (APs) exchanging their signed public keys to create time-stamped location proofs [9]. One subtle issue in processing nearest neighbor queries with this approach is to accurately find all the real neighbors unfortunately is only find approximate neighbors. To find real neighbors, previous work either keeps the proximity of transformed locations to actual locations and incrementally processes nearest-neighbor queries requires trusted third parties to perform location transformation between clients and LBSA servers [10]. In contrast LocX does not trust any third party and the transformed locations are not related to actual locations. Our system is still able to determine the actual neighbors and is resistant against attacks based on monitoring continuous queries [11]. Some existing tracking systems have been known and installed on several OSs of mobile phones. Tracking software on iOS can locate an iPhone iPad and iPod touch, if somebody loses it install the Find My iPhone app on another iOS device launch it and sign in to monitor his or her device's location [12]. As Android occupies the largest smart phone OS market, tracking software on Android platform appears to help the users monitor their devices it works almost the same as the previous location tracking system [13]. We propose a location proof generation and verification scheme which proves the presence of the user within an area of interest at a time and the claim is securely verifiable by LBS. Our mechanism is based on the unique wireless channel characteristics channel state information (CSI) and fuzzy vault, a cryptographic primitive [14]. CSI is the fine-grained physical layer information obtained from 802.11 Wi-Fi packet traces. Fuzzy vault is information theoretically secure scheme in which a user can hide his information by a feature set [15].

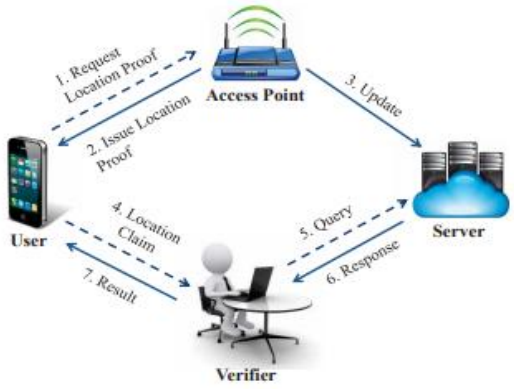

Figure 2. System Model

3. System Model

Few state-of-the-art mechanisms turned their attention to smaller wireless networks wireless LAN to cover indoor environments. The authors have proposed a protocol that allows a mobile device to prove its presence to a Verifier with the help of an AP [16]. The AP the Location Manager measures the round-trip latency of request-reply protocol and based on the time taken for the device to respond, it determines the location. Echo protocol is also based on multiple transmitters and each of the transmitters must measure the round-trip time with a specified precision [17]. Our solution leverages existing Wi-Fi infrastructure is not dependent on any additional entities and does not employ distance

bounding protocol which requires significant changes to the hardware for proof generation. To build a secure location updating module first we utilize a symmetric encryption scheme. We introduce the password-based encryption (PBE) method [18]. It has the feature that the password is set by the user and combines random numbers (salt) to provide the security of data. PBE does not have the concept of secret key because the length of secret key affects the security of method and it is difficult to remember [19].

4. Location Updating

The location updating module is the primary portion of a client responsible for preparing, scheduling, and sending location updates to the cloud end. It is the core function of our tracking system. We provide several mechanisms to ensure three main objectives: (i) the location information sent to the cloud storage should be anonymous and unlikable (ii) forward privacy (stored data on the client should not be sufficient for revealing previous locations); and (iii) searching the storage for updates should be efficient for the owner [20]. To build a secure location updating module, first we utilize a symmetric encryption scheme. We introduce the password-based encryption (PBE) method. It has the feature that the password is set by the user and combines random numbers (salt) to provide the security of data. PBE does not have the concept of secret key because the length of secret key affects the security of method and it is difficult to remember.

The processes of encryption using PBE are as follows:

1. User is asked to set a password when ACT initializes.
2. After ACT collects a location coordinate, the location updating module generates a salt and encrypts the data with the password.
3. ACT sends the ciphertext to the network disk, and the salt will be appended to the location update.
4. After the data packet has been sent, the location and the salt will be erased.
5. When the next location is captured, jump to (2).

We define Si as the state of the mobile device at the time Ti, which contains several elements of ACT: P is the password of ACT, which is for encrypting the location [21]. Li is the location of the mobile device at current time; Ci is the ciphertext, which contains location and time information encrypted; Ri is the salt generated at time Ti, and it will be appended to Ci after it is used for encrypting

5. Location Collection

The location collection module not only obtains the location information of the mobile device but also decides when and how to obtain a location. We provide two modes of location collection: (1) Location collection based on time interval ACT captures a location periodically according to a time interval, which is set by the user. (2) Location collection based on position sensing

5.1. Location collection using global positioning system

Smart phones nowadays are mostly GPS-enabled. More and more applications and services are location-based. Examples of such LBSs include support for finding gas stations and stores with the lowest prices and finding and notifying friends when one arrives at a location, in ACT, location information is the user's privacy and should not be shared with others. Considering a device that may locate itself frequently, the location collection should be concise, efficient, and accurate. There are generally two ways to get location information in Android system: one is through GPS and the other is through network such as Wi-Fi or cellular. GPS has features of high precision, more power consumption, and no network flow generated [22].

5.2. Location updating based on position sensing

As we described before, users' devices usually stay in one place (e.g., home or office) for a long time. Continuous location collection will generate redundant data for storage. Therefore, we recommend the position sensing method because it can save much network traffic and storage space for the user. Now, we explain in detail how it works. When ACT gains the first location, we send it to the network disk and then store it in the memory. After the next location comes, we calculate the distance between the new location coordinate and the former one. If the distance exceeds a threshold, then we think that the device has made an obvious position change [23]. The new location data should be sent to the cloud end; otherwise, we do not send the location because the device may stay in the same place or just move a little distance.

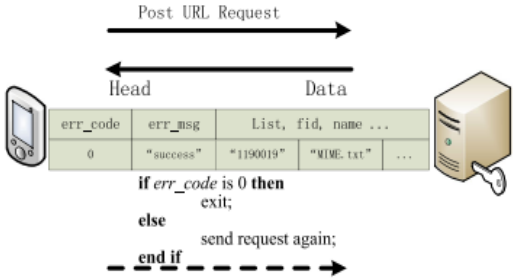

Figure 3. Communication between client and network disk.

6. Global Attestation Scheme

In our model, each device provides reports about their locations. These devices register to our system with their Bluetooth or Wi-Fi MAC addresses and each is given a unique ID. A location report from an entity x does not only contain its location, but also the MAC addresses sensed in the proximity [24]. The report serves as a positive feedback for the trustworthiness of the entity if it complies with the ground truth. Similarly, it serves as a negative feedback if it does not comply with the ground truth. While the computation of positive and negative feedback is trivial when ground truth is available, in our setting, we do not have ground truth for the location of devices. Once a feedback graph is computed we can use existing graph-based trust models to calculate trustworthiness of the nodes in the graph. While various trust models is used in our system, we use two specific graph-based trust models and PeerTrust [25]. These are models that compute global trust values for the nodes a graph based on their local trust values edge weights.

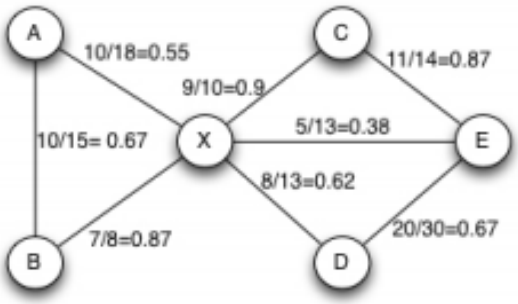

Figure 4. Trust Feedback Graph.

7. Experiments and Results

Mobile device has limited resource compared with ordinary computers; therefore, a lightweight client is necessary for our implementation. The resource consumption consists of three parts: power consumption, storage space requirement and the network traffic We cannot directly measure the power consumption of ACT because it may not be accurate for some factors.

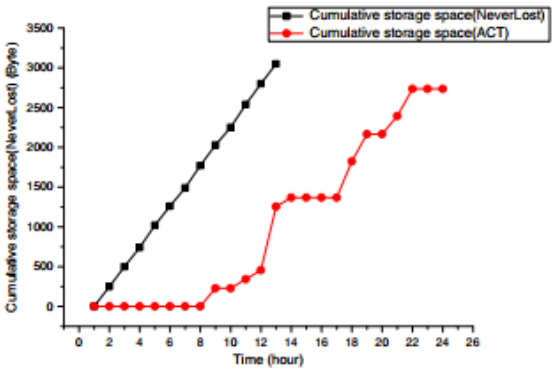

Figure 5. The storage space requirement of Android CLOUD tracker running

To measure the battery overhead of ACT, we conduct experiments as follows: with and without ACT running on the mobile phone. We measure the network traffic that ACT generates when running on a mobile device, which may connect to the Internet via Wi-fi or cellular network, and we care about the network traffic because it is related to user.

8. Conclusion

The PROPS a novel privacy preserving location proof system based on a collaborative architecture. We introduce several mechanisms to achieve both privacy and efficiency in this process and analyze their privacy properties. Using evaluation based on both synthetic and real-world LBSA traces, we find that LocX adds little computational and communication overhead to existing systems. Overall, we also present numerous future works about enhancing ACT system that addresses a range of issues: indoor locating, tamper-evident client, convenient transfer from coordinates to visible locations, transplanting to other platforms, and securely combining tracking with other security mechanisms. Our protocol uses existing Wi-Fi infrastructure and can be implemented by employing commercially available off-the-shelf devices. The time required to generate the location tag in our solution is independent of the size of location tag generated and the distance between the User and AP our scheme is faster by an order of magnitude. In our future work we would like to consider the cases where APs may collude with adversaries to generate a fake location proof and services that may deny access to honest users or grant illegitimate access to dishonest users.

REFERENCES

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

[2] “IEEE Std. 802.11n-2009: Enhancements for higher throughput,” http://www.ieee802.org, 2009.

[3] P. Bahl and V. N. Padmanabhan, “RADAR: An in-building RF-based User Location and Tracking System,” in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), 2000.

[4] S. Brands and D. Chaum. Distance-bounding protocols. In Proceedings of EUROCRYPT ’93. 1993.

[5] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In Proceedings of the 11th ACM conference on Computer and communications security, 2004

[6]. Billion phone dollar bill. lost-and-found/ billion-phone-dollar-bill/ May, 2012

[7]. Apple. MobileMe.

[8] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In Proceedings of the 12th international conference on World Wide Web, pages 640–651. ACM, 2003.

[9] W. Luo and U. Hengartner. Veriplace: a privacy-aware location proof architecture. In ACM GIS, 2010.

[10] G. Ananthanarayanan, V.N. Padmanabhan, L. Ravindranath, and C.A. Thekkath, “Combine: Leveraging the Power of Wireless Peers through Collaborative Downloading,” Proc. Fifth Int’l Conf. Mobile Systems, Applications Services, 2007.

[11] M. Siegler, "Foodspotting is a Location-Based Game that Will Make Your Mouth Water," http://techcrunch.com/2010/03/04/ foodspotting, 2013

[12]. Bergstein B. Mit students show power of open cellphone systems. Associated Press, May 2008. Available from: http://www.usatoday.com/tech/products/2008-05-13-locale-mit_N.htm May, 2012

[13]. Ristenpart T, Maganis G, Krishnamurthy A, Kohno T. Privacy-preserving location tracking of lost or stolen devices: cryptographic techniques and replacing third parties with DHTs. In Proceedings of the 24th USENIX Security Symposium, USENIX, 2008; 275–290

[14] W. Brent and F. Edward, "Secure, Private Proofs of Location," Princeton University, Tech. Rep., 2003, https://www.cs.princeton.edu/research/techreps/TR-667-03.

[15] D. E. Denning and P. F. MacDoran, "Location-based Authentication: Grounding Cyberspace for Better Security," in Computer Fraud and Security, Feb. 1996.

[16] C. Javali, G. Revadigar, W. Hu, and S. Jha, "Poster: Were You in the Cafe Yesterday?: Location Proof Generation & Verification for Mobile Users," in Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys), 2015.

[17] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," Des. Codes Cryptography, vol. 38, no. 2, pp. 237–257, 2006.

[18]. Thiagarajan A, Ravindranath L, Balakrishnan H, Madden S, Girod L. Accurate, low-energy trajectory mapping for mobile devices. In Proceedings of the 8th USENIX conference on Networked Systems Design and Implementation (NSDI'11), Boston, MA, USA, USENIX, 2011; 20–33.

[19]. Becher M. Security of smartphones at the dawn of their ubiquitousness. Ph.D. dissertation, University of Mannheim, Oct. 2009

[20. Hoh B, Gruteser M, Xiong H, Alrabady A. Preserving privacy in GPS traces via uncertainty-aware path cloaking. In Proceedings of the 14th ACM conference on Computer and communications security (CCS'07), New York, NY, USA, ACM, 2007; 161–171.

[21]. Rasmussen K, Capkun S. Location privacy of distance bounding protocols. In Proceedings of the 15th ACM conference on Computer and communications

[22]. Wang S, Min J, Yi B. Location based services for mobiles: technologies and standards. In Proceedings of International Conference on Communication (ICC'08), IEEE, 2008; 35–38.

[23]. MobileMe find my iPhone. Available from: https://me. com/find May, 2012.

[24] L. Xiong and L. Liu. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. Knowledge and Data Engineering, IEEE Transactions on, 16(7):843–857, 2004.

[25] Z. Zhu and G. Cao. Towards privacy-preserving and colluding resistance in location proof updating system. In IEEE Transactions on Mobile Computing, 2011.