International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, 2014
ISSN 2091-2730

Privacy Preserving in a Location Proof Updating System Using Android

B. A. Waghmode[#1], S. Nandgave[*2]

[#]*Student , Department Of Computer Engineering, University of Pune, GHRCOEM, Ahmednagar, Maharashtra, India.*

[*]*Asst. Professor, Department Of Computer Engineering, University of Pune, GHRCEM, Pune, Maharashtra, India.*

[1]bwaghmode15@gmail.com,

[2]sunita.nandgave@raisoni.net

Abstract— Now a day's mobile devices have inbuilt GPS systems such as smartphones and PDAs which plays as increasingly important role in location based services. In location – based applications and services users require proving their locations at a particular time. There are lots of applications in market that helps to track someone's location. As location proof plays a critical role in enabling these applications, they are location – sensitive. The common gain of all these applications is that they offer certain geographical location of a person carrying GPS enabled device. But sometimes users lie about their locations. Location – Based Services (LBS) personalize the service they provide or grant access to resources according to the current location of users. They are used in a variety of contexts, such as real-time traffic monitoring, discount tied to the visit of a particular shop. In most of current schemes, the location of a user/device is determined by the device itself (eg. through GPS) and forwarded to the LBS provider. By doing so, a user can cheat by having his device transmitting a false location to gain access to unauthorized resources, thus raising the issue of verifying the position claimed by a particular user. To counter this threat, LBS should ideally require the requesting device to formally prove that it really is at the claimed location. This notion has been formalized through the concept of location proof which is a proves that someone was at a particular location at a specific moment in time.

Keywords— **Location-based services, location proof, location privacy, pseudonym.**

INTRODUCTION

Nowadays, more and more location based applications and services require users to provide location proofs at a particular time. For example, "Google Latitude" and "Longitude" are two services that enable users to track their friend's locations in real time. These applications are location-sensitive since location proofs plays a critical role in enabling these applications. There are many kinds of location-sensitive applications. One category is location-based access control. For example, a hospital may allow patient information access only when doctors or nurses can prove that they are in a particular room of the hospital [14]. Another class of location-sensitive applications requires users to provide past location proofs [20], such as auto insurance quote in which auto insurance company's offer discounts to drivers who can prove that they take safe routes during their daily commutes, sales officer are roaming out so the organization can track report of their rout and client so they can't cheat with their organization, and location-based social networking in which a user can ask for a location proof from the service requester and accepts the request only if the sender is able to present a valid location proof. The common theme across these location sensitive applications is that they offer a reward or benefit to users located in a certain geographical location at a certain time. Thus, users have the incentive to cheat on their locations.

In general approach, location-sensitive applications require users to prove that really are (or were) at the claimed locations. Although most mobile users have devices capable of discovering their locations, some users may cheat on their locations and there is a lack of secure mechanism to provide their current or past locations to applications and services. One possible solution [11] is to build a trusted computing module on each mobile device to make sure trusted GPS data is generated and transmitted. For example, Lenders et al. [11] proposed such a solution which can be used to generate unforgettable geo tags for mobile content such as photos and video; however, it relies on the expensive trusted computing module on the mobile devices to generate proofs. Although cellular service providers have tracking services that can help verify the locations of mobile users in real time, the accuracy is not good enough and the location history cannot be verified. Recently, several systems have been designed to let end users prove their locations through Wi-Fi infrastructures. For example, Saroiu and Wolman [20] proposed a solution suitable for third-party attestation, but it relies on PKI and the wide deployment of Wi-Fi infrastructure.

In our approach, 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. In APPLAUS, Android mobile devices in range mutually generate location proofs, which are uploaded to an untrusted location proof server than can verify the trust level of each location proof. An authorized verifier can query and retrieve location proofs from the server. Moreover, out location proof

system guarantees user location privacy from every party. More specifically, we use statistically updated pseudonyms at each mobile device to protect location privacy from each other, and from the untrusted location proof server. We develop a user centric location privacy levels in real time and decide whether and when to accept a location proof request.

THE LOCATION PROOF UPDATING SYSTEM

In this section, we introduce the location proof updating architecture, the protocol, and how mobile nodes schedule their location proof updating to achieve location privacy in APPLAUS.

[1] System Architecture:

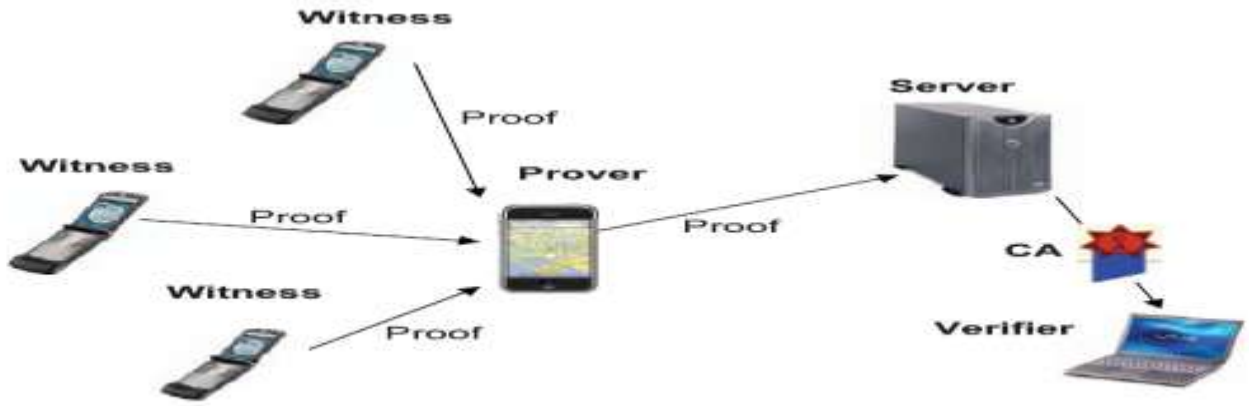

Fig. 1. Location proof updating architecture and message flow.

Prover Module:-

In this module, the node that needs to collect location proofs from its neighboring nodes. When a location proof is needed at time t, the power will broadcast a location proof request to its neighboring nodes through Android. If no positive response is received, the prover will generate dummy location proof and submit it to the location proof server.

Witness for Location:-

Once a neighboring node agrees to provide location proof for the prover, this node becomes a witness of the prover. The witness node will generate a location proof and send it back to the prover.

Location Proof Server:-

As our goal is not only to monitor real-time locations, but also to retrieve history location proof information when needed, a location proof server is necessary for storing the history records of the location proofs. It communicates directly with the prover nodes who submit their location proofs. As the source identifies of the location proofs are stored as pseudonyms, the location proof server is untrusted in the sense that even though it is compromised and monitored by attackers, it is impossible for the attacker to reveal the real source of the location proof.

Certificate Authirity:-

As commonly used in many networks, we consider an online CA which is run by an independent trusted third party. Every mobile node registers with the CA and pre-loads a set of public / private key pairs before entering the network. CA is the only party who knows the mapping between the real identity and pseudonyms (public keys) , and works as a bridge between the verifier and the location proof server. It can retrieve location proof from the server and forward it to the verifier.

Verifier Module:-

A third-party user or an application who is authorized to verify a prover's location within a specific time period. The verifier usually has close relationship with the prover, eg., friends or colleagues, to be trusted enough to gain authorization.

Related Work

Recently, several systems have been proposed to provide end users the ability to provide that they were in a particular place at a particular time. The solution in [2] relies on the fact that nothing is faster than the speed of light in order to compute an upper bound of a user's distance. Capkun and Hubex [3] propose challenge-response schemes, which use multiple receivers to accurately estimate a wireless node location using RF propagation characteristics. In [11], the authors describe a secure localization service that can be used to generate unforgettable geo tags for mobile content such as photos and video. However dedicated measuring hardware or high-cost trusted computing module are required. Saroiu and Wolman [20] propose a solution suitable for third-party attestation, but it relies on a PKI and the wide deployment of Wi-Fi infrastructure. Different from these solutions, APPLAUS uses a peer-to-peer approach and does not require any changes to the existing infrastructure. Smokescreen [4] introduces a presence sharing mobile social service between co-located users which relies on centralized, trusted brokers to coordinate anonymous communication between strangers. SMILE [15], [16] allows users to establish missed connections and utilizes similar wireless techniques to prove if a physical encounter occurred. However, this service does not reveal the actual location information to the service provider thus can only provide location proofs between two users who have actually encountered. APPLAUS can provide location proofs to third-party by uploading real encounter location to the untrusted server while maintaining location privacy. There are lots of existing works on location privacy in wireless networks, in [8], the authors propose to reduce the accuracy of location information along spatial and / or temporal dimensions. This basic concept has beed improved by a series of works [7], [10]. All the above techniques cloak a node's locations with its current neighbors by trusted central servers which is vulnerable to DoS attacks or to be compromised. Different from them, our approach does not require the location proof server to be trustworthy. Xu and Cai [23] propose a feeling-based model which allows a user to express his privacy requirement. One important concern here is that the spatial and temporal correlation between successive locations of mobile nodes must be carefully eliminated to prevent external parties from compromising their location privacy. The techniques in [1], [6] achieve location privacy by changing pseudonyms in regions called mix zones. In this paper, pseudonyms of each node are changed by the node itself periodically following a Poisson distribution, rather than being exchanged between two untrusted nodes. Identifying a fundamental tradeoff between performance and privacy, Shao et al. [21], [24] propose a notion of statistically strong source anonymity in wireless sensor networks for the first time, while Li and Ren [13] and Zhang et al. [25] tried to provide source location privacy against traffic analysis attacks through dynamic routing or anonymous authentication. Our scheme uses similar source location unobservability concept in which the real location proof message is scheduled through statistical Algorithms. However, their focus is to generate identical distributions between different nodes to hide the real event source, while our focus is to design distinct distributions between different pseudonyms to protect the real identity.

ACKNOWLEDGMENT

We would like to sincerely thank Prof. Mrs. Sunita Nandgave, our mentor (Asst. Professor, GHRCEM, Wagholi, Pune), for her support and encouragement.

CONCLUSION

APPLAUS uses Android mobile devices mutually generate location proofs and upload to the location proof server. This may be the first work to address the joint problem of location proofs effectively, and it preserves source location privacy and its collusion resistant.

REFERENCES:

[1] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Security and Privacy, 2003.
[2] S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc. Workshop Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '93), 1994.
[3] S. Capkun and J.-P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," Proc. IEEE INFOCOM, 2005.
[4] L.P. Cox, A. Dalton, and V. Marupadi, "SmokeScreen: Flexible Privacy Controls for Presence-Sharing," Proc. ACM MobiSys, 2007.
[5] N. Eagle and A. Pentland, "CRAWDAD Data Set mit/reality(v.2005-07-01)," http://crawdad.cs.dartmouth.edu/mit/reality, July 2005.
[6] J. Freudiger, M.H. Manshaei, J.P. Hubaux, and D.C. Parkes, "On Non-Cooperative Location Privacy: A Game-Theoretic Analysis," Proc. 16th ACM Conf. Computer and Comm. Security (CCS), 2009.
[7] B. Gedik and L. Liu, "A Customizable K-Anonymity Model for Protecting Location Privacy," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), 2005.
[8] M. Gruteser and D. Grunwald, "Anonymous Usage of Location- Based Services through Spatial and Temporal Cloaking," Proc. ACM MobiSys, 2003.
[9] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.C. Herrera, A.M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring," Proc. ACM MobiSys, 2008.
[10] T. Jiang, H.J. Wang, and Y.-C. Hu, "Location Privacy in Wireless Networks," Proc. ACM MobiSys, 2007.
[11] 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.
[12] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy," Proc. Fifth ACM Workshop Privacy in Electronic Soc., 2006.
[13] Y. Li and J. Ren, "Source-Location Privacy Through Dynamic Routing in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2010.
[14] W. Luo and U. Hengartner, "Proving Your Location Without Giving Up Your Privacy," Proc. ACM 11th Workshop Mobile Computing Systems and Applications (HotMobile '10), 2010.
[15] J. Manweiler, R. Scudellari, Z. Cancio, and L.P. Cox, "We Saw Each Other on the Subway: Secure Anonymous Proximity-Based Missed Connections," Proc. ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile '09), 2009.
[16] J. Manweiler, R. Scudellari, and L.P. Cox, "SMILE: Encounter- Based Trust for Mobile Social Services," Proc. ACM Conf. Computer and Comm. Security (CCS), 2009.
[17] F.J. Massey Jr., "The Kolmogorov-Smirnov Test for Goodness of Fit," J. Am. Statistical Assoc., vol. 46, no. 253, pp. 68-78, 1951.
[18] I. Rhee, M. Shin, K. Lee, and S. Chong, "On the Levy-Walk Nature of Human Mobility," Proc. IEEE INFOCOM, 2007.
[19] J.L. Romeu, "Kolmogorov-Simirnov: A Goodness of Fit Test for Small Samples," START: Selected Topics in Assurance Related Technologies, 2003.
[20] S. Saroiu and A. Wolman, "Enabling New Mobile Applications with Location Proofs," Proc. ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile '09), 2009.
[21] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, 2008.
[22] A. Wald, Sequential Analysis. Dover, 2004.
[23] T. Xu and Y. Cai, "Feeling-Based Location Privacy Protection for Location-Based Services," Proc. 16th ACM Conf. Computer Comm. Security (CCS), 2009.
[24] Y. Zhang, W. Liu, and W. Lou, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005