International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

# A Survey on Security and Privacy Based Location Based Recompense Scheme

**Prema. S. Patil (Wankhede) [1], M. K Kodmelwar[2]**

[1] Department of Computer Engineering, BSCOER Narhe, Pune, University of Pune, Maharashtra, India

[2]Assistant Professor, Department of Computer Engineering, BSCOER Narhe, Pune, University of Pune, Maharashtra, India

**Abstract:** ***The creation of mobile devices has directed the mobile advertising to flow in the past few years. Developing as a new type of mobile advertising, mobile location-based services have elaborate intense consideration in recent times. Inappropriately, existing mobile location-based services have a lot of limitations and rise many concerns, particularly about system security and user. In this paper, we put forward a new location based rewarding system, where mobile users can gather location-based tokens from token distributors, and then redeem their collected tokens at token collectors for beneficial rewards. Tokens act as real-world currency. The token distributors and collectors can be any marketable entities or merchants that request to interest customers through such a promotion system, such as cafés, stores. We develop a security and privacy responsive location-based rewarding protocol for the system, and show the inclusiveness and reliability of the procedure. Moreover, we show that the system is robust to several attacks and mobile users' confidentiality can be well protected in the period in-between. We finally implement the structure and performance extensive experimentations to validate the system productivity in terms of working out, announcement.***

**Keywords:** Mobile location based services, confidentiality, and security.

## 1. Introduction

Location-Based Rewarding System contains of a trusted third party, mobile user, token distributor, token collector, and a central controller. The trusted third party difficulties every mobile users with actual identity and a resultant certificate. A mobile user is capable to achieve a location-based token when it visits a commercial entity that takes part in the system. The issue tokens at numerous token distributors have the similar format but maybe different indicated values. With all the collected tokens, mobile users can redeem them for advantageous rewards not only at the same store, but also at any other vender entities, i.e., TCs, that have combined the system. The amount of established rewards hinge on the value represented by the collected tokens. Besides, the central stores token audition info sent by token distributors and provides it to TCs when required. We design a security and privacy aware location based rewarding protocol for the proposed system. The protocol is composed of three parts identity introduction, token supply, and token reclamation. Completeness means that honest mobile Users can always successfully obtain tokens from token distributors and redeem valid tokens at token collectors. Security raises to that the possibility that forged/tampered/stolen tokens can be redeemed is insignificant.Mobile user individual at a like actual uniqueness, token info together with the worth of a token, and location histories

Then, we design a security and privacy alert location based rewarding protocol for the forthcoming system. We income on that TDs, token collector, and the CC work in The semi reliable mode, i.e., they reliably and appropriately execute the system procedure but are curious about MU confidentiality, with their individual information like actual identities, token info, and location histories. The TTP issues each MU with an individuality and different certificate. All mobile user keeps its identity private and generates a new pseudonym for each token request or redemption. The certificate is used for a user's identity authentication without revealing its real identity. Token distributor needs to verify if an MU requesting a token is a legal user in the system without knowing its real ID. After that, the token distributor issues the MU with an anonymous token which can be redeemed at any token collector for rewards. Since the token contains some of the MU's private information, it is only kept by the MU but not any other network entities, including token collector and the CC. The token distributor then generates corresponding audition information for the token and sends it instead of the token itself to the CC for future token verification.

In token redemption, a token collector first verifies whether the current MU trying to redeem a token is a legal system user, without knowing its real ID. Then, the token collector checks to see if the token to be redeemed is intact and has not been tampered since it was generated with the service of the CC, without significant the contented of the token. After that, the token collector checks if the token does belong to the MU. If the MU passes all these verification phases, the token collect or verifies whether the value of the token claimed by the MU is accurate, and if so, allocates the consistent reward to him/ her. Consequently, in our future system, no unique else other than the TTP can know an MU's real identity. As the CC and token collector only have the knowledge of token audition information, they do not know the content of any token.

Since a token collector / token distributor is only aware of the location of the tokens it issued/accepted and there is no central server to store all the historical location information, no entity could figure out any specific MU's location history.

## 2. Literature Review

Mobile location-based services (MLBSs) have performed as a new type of mobile advertising. The rapid growths of mobile devices, mobile location based service have occurred as a new kind of mobile promotion According to a 2010 reported by Pew Research Center, on some specified day, 1 percent of online Americans used MLBSs [1]. Juniper Research expects that the proceeds from mobile location based service will flow to more than $12.7 billion by 2014 [2]. Presently, there are several types of mobile location based service. One of these location based social networking, such as Facebook Places [3]. Additional kind of mobile location based service call for the users to deliver present or historical location proof to achieve some resolutions [4], [5], [6]. Mobile business is alternative division of MLBSs, for example, forwarding advertisements to customers when they are near a business advertisement [7]. These mobile location based service do not deliberate rewarding services.

Further in recent times, a new form of mobile location based service named location based check in game, which is established based on location based social networking, lets users get advantageous rewards if they visit certain places. In specific, certain applications, together with Foursquare [8], and Loopt Star [9], let users patterned in different locations to not only participate with friends in games, but also receive rewards, or discounts from sellers and administrations. The rewards and reward expanses can be diverse depending on time of day, how repeatedly the person has checked it in the previous, and so on. However, these location based check in systems are incomplete in several aspects. Major customers can only collect and trade in rewards at the same variety stores or even the same store only. For example, if customer appointments a Gap store twice, he/she can become a discount on the purchases at Gap stores only, not at any other places like Starbucks. This importantly deteriorates the customers' motivations for visiting the locales. Another, from a service provider's outlook, security is not assured in the current systems. Since users can be given profits for visiting several locations, they have encouragements to privilege that they are at certain locations even all the same they are not. Most of those location based check in applications use the GPS on a user's mobile device to verify the location claimed by the user. This problem is in fact very common in most MLBSs and have not been reasonably resolved by up-to-date works [5],[6], [11], [12], [13]. Another, from Mobile users' viewpoint, Mobile users' privacy with identity privacy and location privacy has been mostly overlooked in the current systems. In specific, since the current systems use central servers to store all mobile users' accounts, they can certainly recognize which mobile users have always been to which spaces at what periods for what purposes. Previous mechanisms on user individuality privacy in wireless networks are not appropriate to, mobile location based service scenarios [14], [15]. While there has been several examination on location privacy concerning general location based services, such as k-anonymity cloaking [16], [17], [18], [19], location confusion [20], [21], [22], [23], [24], fictitious name exchanges in mix regions [25], [26], [27], [28],they entirely have their boundaries. Note that our strategy does not involve any responsible server for generating/Storage location proofs like in [3], [5], [8], [13], [29] or for defensive user location privacy like in [16], [17], [19] [25] [27]. Furthermore, we have proved both the fullness and the dependability of the protocol, while most Earlier systems only focus on their completeness.

What's more, we study the security and privacy of the LocaWard system. We discover that the system is robust to numerous attacks such as multi token request attack, duplicate token restoration attack, takeoff attack, token altering attack, and colluding attack. We similarly show that the mobile user privacy can be well protected. In accumulation, we form a recognized containing of an Android Smartphone and a laptop to appliance our future system. We authenticate the effectiveness of LocaWard in relationships of computation, communication, energy consumption, and storage costs concluded broad research.

## 3. Propose Work

The proposed system is capable to resilient various attacks and mobile user privacy can be well protected. Also for the security purpose in our system the trusted third party who initially authenticate or registered the mobile users trace the IMEI number of the mobile user. When the mobile user request for the token to the token distributors, token distributor checks the IMEI number of the mobile user, token collector also checks the IMEI number of the mobile user when mobile user request for token to the token collector. In the proposed system we detect an attack by tracing the IP address of the attacker. The security and privacy of the LocaWard system. We discover that the system is robust to numerous attacks such as multi token request attack, duplicate token restoration attack, takeoff attack, token altering attack, and colluding attack. We similarly show that the mobile user privacy can be well protected.

This system can be developed to implement a new type of mobile marketing, mobile location-based services (MLBSs). The user may be general users. It considers that they have basic knowledge of using computer programming and basic understanding about Loca Ward system. The system gives the output in the form of tokens, token rewards, etc. The proposed system consists of a trusted third party (TTP), mobile users (MUs), token distributors (TDs), token collectors (TCs), and a central controller (CC). At the time of registration user's IMEI number is traced by the TTP and this IMEI number is saved in database and for authentication.

## 4. System Architecture

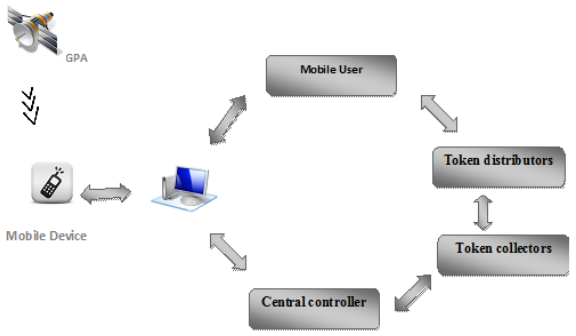


**Figure 1:** System Architecture

## 5. Conclusion

In this paper we have discussed about a secure, privacy conserving, and realistic location-based rewarding system. We have designed a security and privacy aware protocol for the system and recognized its completeness and soundness. We find that the system is resistant to many types of attacks and mobile users' privacy can be well protected. We have also estimated the system effectiveness by general real try out and show that the system working out communication, energy, and storage costs are low. Furthermore, while the wished-for security and privacy aware location-based rewarding protocol is for our system, the procedures in this can be generalized to address security and privacy problems in overall location based services and other areas.

## References

[1] http://pewinternet.org/~/media/Files/Reports/2010/PIP-Location%20based%20services.pdf, 2010.
[2] Juniper Research, Mobile Location Based Services Applications, Forecasts and Opportunities 2010-2014,https://www.juniperre search.com/reports/mobile location_based_services, 2010.
[3] http://www.facebook.com/about/location.
[4] W. Luo and U. Hengartner, "Proving Your Location without Giving up Your Privacy," Proc. 11th Workshop Mobile Computing Systems Applications, Feb. 2010.
[5] S. Saroiu and A. Wolman, "Enabling New Mobile Applicationswith Location Proofs," Proc. 10th Workshop Mobile ComputingSystems Applications, Feb. 2009.
[6] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi,"Location-Based Trust for Mobile User-Generated Content:Applications, Challenges and Implementations," Proc. NinthWorkshop Mobile Computing Systems Applications (HotMobile '08), Feb. 2008.
[7] S. Loreto, T. Mecklin, M. Opsenica, and H.-M.Rissanen, "ServiceBroker Architecture: Location Business Case and Mashups," IEEEComm. Magazine, vol. 47, no. 4, pp. 97-103, Apr. 2009.
[8] https://foursquare.com/.
[9] http://www.loopt.com/about/tag/loopt-star/.
[10] Z. Zhu and G. Cao, "Towards Privacy Preserving and CollusionResistance in Location Proof Updating System," IEEE Trans.Mobile Computing, vol. 12, no. 1, pp. 51-64, Nov. 2011.
[11] B. Waters and E. Felton, "Secure, Private Proofs of Location,"Technical Report TR-667-03, Dept. of Computer Science, PrincetonUniv., Jan. 2003.
[12] N. Sastry, U. Shankar, and D. Wagner, "Secure Verification ofLocation Claims," Proc. Second ACM Workshop Wireless Security(WiSe '03), Sept. 2003.
[13] W. Luo and U. Hengartner, "Veriplace: A Privacy-Aware LocationProof Architecture," Proc. 18th SIGSPATIAL Int'l Conf. AdvancesGeographic Information Systems (GIS '10), Nov. 2010.
[14] K. Ren and W. Lou, "A Sophisticated Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless MeshNetworks," Proc. 28th Int'l Conf. Distributed Computing Systems(ICDCS '08), June 2008.
[15] C. Ardagna, S. Jajodia, P. Samarati, and A. Stavrou, "ProvidingMobile Users' Anonymity in Hybrid Networks," Proc. 15thEuropean Symp. Research Computer (ESORICS), Sept. 2010.
**[16]** M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," Proc.First Int'l Conf. Mobile Systems, Applications Services (Mobisys '03),May 2003.
[17] B. Gedik and L. Liu, "Protecting Location Privacy with PersonalizedK-Anonymity: Architecture and Algorithms," IEEE Trans.Mobile Computing, vol. 7, no. 1, pp. 1-18, Jan. 2008.
[18] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "PreventingLocation-Based Identity Inference in Anonymous SpatialQueries," IEEE Trans.Knowledge Data Eng., vol. 19, no. 12,pp. 1719-1733, Dec. 2007.
[19] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: APersonalized Anonymization Model," Proc. IEEE 25th Int'l Conf.Distributed Computing Systems (ICDCS), June 2005.
[20] H. Kido, Y. Yanagisawa, and T. Satoh, "An AnonymousCommunication Technique Using Dummies for Location-BasedServices," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems(ICDCS), July 2006.
[21] H. Lu, C.S. Jensen, and M.L. Yiu, "Pad: Privacy-Area Aware,Dummy-Based Location Privacy in Mobile Services," Proc. ACMSeventh ACM Int'l Workshop Data Eng. Wireless Mobile Access(MobiDE), June 2008.
[22] M. Duckham and L. Kulik, "A Formal Model of Obfuscation andNegotiation for Location Privacy," Proc. Int'l Conf. PervasiveComputing, May 2005.
[23] C.A. Ardagna,M. Cremonini, S.D.C. di Vimercati, and P. Samarati,"An Obfuscation-Based Approach for Protecting Location Privacy,"IEEE Trans. Dependable Secure Computing, vol. 8, no. 1, pp. 13-27, Jan. 2011.
[24] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "Cap: AContext-Aware Privacy Protection System for Location-BasedServices," Proc. IEEE 29th Int'l Conf. Distributed Computing Systems(ICDCS '09), June 2009.
[25] A. Beresford and F. Stajano, "Location Privacy in PervasiveComputing," IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55,Jan.-Mar. 2003.
[26] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "PreservingPrivacy in Gps Traces via Uncertainty-Aware Path Cloaking,"Proc. 14th ACM Conf. Computer Comm. Security (CCS '07), Jan. 2007.
[27] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-Aware Multiple Mix Zone Placement for Protecting LocationPrivacy," Proc. IEEE INFOCOM, Mar. 2012.
[28] J. Meyerowitz and R.R. Choudhury, "Hiding Stars with Fireworks: Location Privacy through Camouflage," Proc. ACMMobiCom, Sept. 2009.
[29] http://www.yelp.com/, 2012