International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Secured Location-Based Rewarding System Using Digital Signature (SLBRDS)

Rubina Ashfaque Shah[1], Dr. Rahat Khan[2]

[1]Department of Computer Science and Engineering Marthawada Shikshan Prasark Mandal's Deogiri Institute of Engineering & Management Studies, Aurangabad Maharashtra state, India 2015-16

[2]Associate Professor Department of Computer Science and Engineering Marthawada Shikshan Prasark Mandal's Deogiri Institute of Engineering & Management Studies, Aurangabad Maharashtra state, India 2015-16

Abstract: ***In the past few years the research of mobile devices has motivated the mobile marketing to surge. In recent few years the new type of mobile marketing term as mobile location based services has attracted strong attention. Regrettably, current MLB techniques have a lot of limitations and raise many concerns, especially about the security and privacy of the system. Here we proposed a novel location based rewarding system which termed as SLBRDS. In this system mobile user can gather area based tokens from the token wholesalers, and then exchange their collected tokens at token collectors for beneficial rewards. Here, we develop a security and privacy aware location based rewarding protocol for the SLBRDS system, Furthermore, we also show that the proposed system is capable to flexible different attacks and versatile client security can be well protected. Also for the security purpose in our framework the trusted third party who at first authenticate or register the mobile users trace the digital signature of the mobile user. When the mobile user request for the token to the token distributors, token distributor checks the digital signature of the mobile user, token collector also checks the digital signature of the mobile user when versatile client demand for token to the token gatherer.***

Keywords: Mobile Location-Based Services, Security, Privacy, Digital Signature. Recoverable

1. Introduction

In recent few years the new type of mobile marketing term as mobile location based services has attracted strong attention. Regrettably, current MLB techniques have a lot of limitations and raise many concerns, especially about the security and privacy of the system. Here we propose a realistic location based rewarding system which termed as SLBRDS. In this system mobile client can gather location based tokens from the token distributors, and then exchange their collected tokens at token collectors for beneficial rewards. Here we develop a security and privacy aware location based rewarding protocol for the SLBRDS structure, and demonstrates the result and soundness of the protocol. Moreover, we also demonstrates that the proposed framework is capable to resilient various attacks and mobile user privacy can be well protected. Also for the security reason in our framework the trusted third party who initially authenticate or registered the mobile users trace the digital signature of the mobile user. When the mobile user request for the token to the token distributors, token distributor checks the digital signature of the mobile user, token collector also checks the digital signature of the mobile client when mobile client demand for token to the token collector. Propose system detects an attack by tracing the IP address of the attacker.

All the more as of late, another sort of MLBSs called location based registration amusement, which is produced in light of area based person to person communication lets clients procure gainful prizes on the off chance that they visit certain spots. Specifically, a few applications, including Foursquare and Loopt Star let clients check in diverse areas (e.g., coffeehouses, eateries, shopping centers) to contend with companions in recreations, as well as acquire remunerates, focuses, or rebates from retailers and associations. The prizes and remunerate sums can be distinctive relying upon time of day, how habitually the individual has checked it previously, etc. On the other hand, these area based registration frameworks are restricted in a few perspectives. First of all, customers can just get and reclaim rewards at the same brand stores or even the same store just. For example, if a client visits a Gap store twice, he/she can get a markdown on the buys at Gap stores (or the same Gap store) just, not at some other spots like Starbucks. This significantly debilitates the clients' inspirations for going to the regions. Second, from an administration supplier's point of view, security is not ensured in the current frameworks. Since clients can get advantages for going by a few spots, they have motivations to assert that they are at sure areas despite the fact that they are most certainly not. The greater part of those area based registration applications (e.g., Foursquare) is that they utilize the GPS on a client's cell phone to check the area guaranteed by the client. In any case, clients may undermine their areas by, for instance, jail breaking their cell phones. This issue is truth be told extremely basic in many MLBSs and have not been attractively tackled by existing works. Third, from clients' point of view, clients' protection including character security and area security has been to a great extent overlooked in the present registration frameworks. Specifically, since the present frameworks use focal servers to store every one of clients' records, they can without much of a stretch know which clients have ever been to which puts at what times for what purposes.

2. Proposed Methodology

In this paper, a privacy-saving, and realistic mobile location-based rewarding framework, called Secured Location-Based

Rewarding System using digital signature which endeavors to address the above concerns is proposed. The proposed framework comprises of a trusted third party (TTP), mobile users (MUs), token distributors (TDs), token collectors (TCs), and a central controller (CC). The TTP issue every MU with an actual personality and a relating certificate. A legal MU has the capacity obtain a location-based token when it visits a commercial element that participates in the framework, i.e., a TD. The issued tokens at a choice of TDs have the similar set-up yet perhaps diverse indicated values. With all the gathered tokens, a MU can reclaim them for beneficial rewards not just at the same store or brand stores, additionally at any different retailers or commercial elements, i.e., TCs that have joined the framework. The amount of rewards relies upon the value of customer collected tokens. Moreover, the CC stores token audition information sent by TDs and gives it to TCs when required.

We assume that TDs, TCs, and the CC work in the semi honest mode, i.e., they faithfully and effectively execute the framework convention however are interested about MUs privacy, including their personal information like real characters, token information, and location histories. Specifically, the protocol is made out of three parts: personality initiation, token dissemination, and token recovery. In personality initiation, the TTP issues each MU with the identity and a relating certificate. The certificate is utilized for a client's identity authentication without revealing its real personality. In token conveyance, a TD needs to confirm if a MU asking for a token is a legal client in the framework without knowing its real ID. After that, the TD issues the MU with an anonymous token which can be recovered at any TC for rewards. Since the token contains a portion of the MU's private information, it is just kept by the MU and not any other system elements, including TCs and the CC. The TD then generates relating trial information for the token and sends it in its place of the token itself to the CC for future token verification. In token reclamation, a TC first checks whether the present MU attempting to reclaim a token is a legal framework client, without knowing its real ID. At that point, the TC verifies whether the token to be reclaimed is intact and has not been tampered since it was generated with the assistance of the CC, without knowing the substance of the token. After that, the TC checks if the token belongs to the MU. In the event that the MU passes all these verification phases, the TC checks whether the value of the token claimed by the MU is genuine, and assuming this is the case, appropriates the relating rewards to him/her. In this way, in our proposed framework, nobody else other than the TTP can know a MU's real identity. As the CC and TCs just have the token audition information, they don't have the foggiest idea about the substance of any token. Since a TD/TC is just aware of the location of the tokens it issued/accepted and there is no essential server to store all the chronological location information, no element could make sense of any particular MU's location history.

Plus, We analyze the security and privacy of the Secured Location-Based Rewarding System using Digital Signature (SLBRDS) framework. We come to that the framework is adaptable to various attacks, for example, multi-token request attack, duplicate token redemption attack, impersonation attack and token tampering attack. We also demonstrate that the MUs privacy can be all around secured. In addition, here we evaluate the computation, communication, energy, and storage costs of the proposed SLocaWard system on our testbed, which consists of a laptop and an Android Smartphone. In particular, the laptop has a 2.5 GHz CPU and 2 GB RAM, while the Smartphone is a Samsung Nexus S with 1 GHz ARM Cortex A8 processor and 512 MB RAM. We implement a TD, a TC, and the CC on the laptop platform, and a MU on the Smartphone platform, respectively. The two platforms communicate with each other via the WiFi, and their conversations are carried out via TCP connections. Thus, considering that TDs/TCs may be connected to their access points via cables.

3. Performance Analysis

In this section, we present more experiment results in terms of computation, communication, energy, and storage costs. The notations for the operations involved in the proposed protocol are also shown in Table 1.

Table 1: Operation Notation

Operations	Description
$Pair_{\mathbb{G}}$	Pairing $e(g,h)$, where $g,h \in \mathbb{G}$
$Exp_{\mathbb{G}}$	Exponentiation g^a, where $g \in \mathbb{G}$
$Hash_{\mathbb{G}}$	Hash values to group $\mathbb{G}$
Mul	Multiplication
Enc/Dec	Encryption/Decryption
Add	Addition
XOR	Exclusive or

3.1 Efficiency of Token Distribution – Single Token Request

Here, we show the detailed computation, communication, and energy consumption costs in the token distribution process in Table 2, Table 3, and Table 4, respectively, in the case of only one single token request.

Table 2: Computation Time in the Token Distribution Process.

Computation Time (ms)	MU	TD	Total
Identity Authentication	2.73	2.52	5.25
Token Distribution	0.45	0.69	1.14

Table 3: Communication Cost in the Token Distribution Process.

Identity Authentication	MU	TD	Total
Payload Size (bytes)	512	256	768
Communication Time (ms)	168.39	111.48	279.87
Token Distribution	MU	TD	Total
Payload Size (bytes)	0	320	320
Communication Time (ms)	0	59.32	59.32

Table 4: Energy Consumption of the MU in Token Distribution Process

Token Distribution Process	Energy Consumption at MU (mAh)
Identity Authentication	0.84
Token Distribution	0.15
Total	0.99

3.2 Efficiency of Token Distribution – Multiple Token Requests

In this section, we show the detailed computation, communication, and energy consumption costs in the token redemption process in Table 5, Table 6, and Table 7, respectively, in the case of one single token redemption request. Note that although the dominant computation complexity in the reward distribution phase at the TC and that in the identity authentication phase at the TC/TD are the same, i.e., $2\times Exp$, the computation time in the former case, *i.e., 20.62 ms*, is much larger than that in the latter case, i.e., *2.95 ms*. This is because we have to use a special function in jPBC to perform *Exp* in the reward distribution phase due to other paring operations. It is less efficient than the function use in the identity authentication phase.

Table 5: Computation Time in the Token Redemption Process.

Computation Time (ms)	MU	TD	Total
Identity Authentication	2.8	2.95	5.75
Token Audition	0.67	218.75	219.42
Token Property Validation	0	22.5	22.5
Reward Distribution	0.47	20.62	21.09

3.3 Efficiency of Token Redemption – Multiple Token Requests

Next, the experiment results are illustrated when there are multiple MUs redeeming their tokens, which are simulated by one smart phone. The time between two adjacent arriving MUs is assumed to follow the exponential distribution with parameter λ2. Besides, each MU can redeem multiple obtained tokens. In the experiment, let all MUs have the same number of tokens, which is denoted by N.

Table 6: Communication Cost in the Token Redemption Process.

Identity Authentication	MU	TC	Total
Payload Size (bytes)	512	256	768
Communication Time (ms)	166.24	112.75	278.99
Token Audition	MU	TC	Total
Payload Size (bytes)	64	256	300
Communication Time (ms)	56.13	58.45	114.58
Token Property Validation	MU	TC	Total
Payload Size (bytes)	0	0	0
Communication Time (ms)	0	0	0
Reward Distribution	MU	TC	Total
Payload Size (bytes)	32	0	32
Communication Time (ms)	55.97	0	55.97

Table 7: Energy Consumption of the MU in the Token Redemption Process

Token Redemption Process	Energy Consumption at MU (mAh)
Identity Authentication	0.89
Token Audition	0.34
Token Property Validation	0
Reward Distribution	0.25
Total	1.48

4. Security Analysis

First we analyze the security of the system, considering that all the misbehaving MUs have valid identities issued by the TTP. Note that those MUs who do not have valid identities can be detected at the identity authentication phase.

4.1. Multi-token request attack

When visiting a TD, a well behaved MU should obtain only one location-based token during each predefined time window, while a misbehaving MU may generate excessive token requests either by the same user ID or by different user IDs, and try to get more than one tokens. Recall that an MU is required to send certificate during the identity authentication at the TD, and certificate is unique for every MU. By checking the existing request records in the time window for duplicate user IDs or certificate's the TD can easily detect any multitoken request attack.

4.2. Duplicate token redemption attack

In the duplicate token redemption attack, a misbehaving MU may try to redeem the same token multiple times. This kind of misbehavior can be easily defended against in our SLocaWard system. The redemption flag of a token kept at the CC would be set to (or the token can be deleted by the CC permanently), after the token is redeemed for the first time. Then, when the same token is redeemed again (i.e., indexed by the same user ID), the TC would check with the CC and can easily find out that this is a duplicate redemption.

4.3. Impersonation attack

An impersonation attack is that a misbehaving MU manages to steal another MU's user ID, or certificate, or both to obtain tokens, or to steal another MU's tokens, in order to obtain more rewards from a TC. This scheme is also efficient in defending against such misbehavior. In particular, in the first case, i.e., when a misbehaving MU uses another MU's user ID and/or certificate, to request for tokens, it cannot pass the identity authentication at the TD, since it does not know that MU's real identity. In the second case, i.e., when an MU tries to redeem a stolen token, it cannot pass the identity authentication phase at the TC for the same reason. Besides, even if an MU could forge a redemption token request with its own certificate and the user ID in a stolen token, it would fail the token property validation.

4.4. Token-tampering attack

In a token-tampering attack, a misbehaving MU tries to forge a fake token, or to change certain content, for example, value, of a token to get beeficial rewards. In the first case, since a forged token is not obtained from a TD, there will not be any related records at the CC. Thus, when the misbehaving MU tries to redeem the forged token at a TC, the TC can find out that there is no corresponding audition information for this token at the CC during the token audition phase and will abort the redemption process. In the second case, if MU tampers any content of the token, this token cannot pass the

token audition, as shown in the soundness of the token audition phase.

5. Comparison

No.	*Approach*	*Advantage*	*Disadvantage*
1	Location obfuscation	Allow users to express their privacy preferences	Degraded quality of service to user
2	APPLAUS	Provides location proofs effectively also preserves the source privacy	Computation time is costly and colliding attacks detection ratio is low
3	Oblivious Transfer and PIR	Computationally and also in communication more efficient	The overhead of the primality test is larger
4	IClique Cloak	Effectively prevent location-dependent attacks when locations are updated	The cost for location dependent attacks is small
5	LocaWard	Resilient to various attacks such as multi token request attack	Do not provide security to general LBS
6	SLBRDS	Authenticating the secure key using digital signature, privacy preserving and recoverable system.	Prevention from the active attack is not possible.

6. Conclusion

A secure, privacy preserving, and realistic location-based rewarding system, SLocaWard has been proposed. The system is resilient to many types of attacks and mobile user's privacy can be well protected as well. After going through the surveying, it can be gathered that there is a huge scope of application development in mobile domain. And our best efforts are try to implement this application on the Apple phones also. And try to provide some live advertisement / notification to users.

7. Acknowledgement

I would like to place on record my deep sense of gratitude to **Prof. S. B. Kalyankar**, HOD-Dept. of Computer Science and Engineering, Deogiri Institute of Engineering and management Studies Aurangabad, for his generous guidance, help and useful suggestions.

I am extremely thankful to **Dr. Ulhas Shiurkar**, Director, Deogiri Institute of Engineering and management Studies Aurangabad, for providing me infrastructural facilities to work in, without which this work would not have been possible.

Expression of gratitude and thankfulness for providing standard database for the completion of the said task with name of the database providers.

References

[1] JPJ1438-LocaWard A Security and Privacy Aware Online].Available: http://www.mediafire.com/view/8crrkj1ee7t9keo/JPJ1438%20%20LocaWard%20A%20Security%20and%20Privacy%20Aware.pdf [Accessed 15 September 2015].
[2] Pew Research Center: Internet, Science & Technology [Online]. Available: http://pewinternet.org/~/media/Files/Reports/2010/PIP-Location%20based%20services.pdf, 2010. [Accessed 3 November 2015].
[3] Juniper Research, Mobile Location Based Services Applications, Forecasts and Opportunities 2010-2014, [Online]. Available:
[4] https://www.juniperre search.com/reports/mobile location_based_services, 2010. [Accessed 5 November 2015].
[5] Facebook - Log In or Sign Up [Online]. Available:
[6] http://www.facebook.com/about/location. [Accessed 5 November 2015].
[7] W. Luo and U. Hengartner, *"Proving Your Location without Giving up Your Privacy,"* Proc. 11th Workshop Mobile Computing Systems Applications, Feb. 2010.
[8] S. Saroiu and A. Wolman, *"Enabling New Mobile Applicationswith Location Proofs,"* Proc. 10th Workshop Mobile ComputingSystems Applications, Feb. 2009.
[9] 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 Applications (HotMobile '08), Feb. 2008.
[10] 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.
[11] Foursquare Labs, Inc. [US]. [Online]. Available: https://foursquare.com/. [Accessed 5 November 2015].
[12] Loopts Labs, [Online]. Available: http://www.loopt.com/about/tag/loopt-star/. [Accessed 5 November 2015].
[13] 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.
[14] B. Waters and E. Felton, *"Secure, Private Proofs of Location,"*Technical Report TR-667-03, Dept. of Computer Science, PrincetonUniv., Jan. 2003.
[15] N. Sastry, U. Shankar, and D. Wagner, "*Secure Verification ofLocation Claims,"* Proc. Second ACM Workshop Wireless Security(WiSe '03), Sept. 2003.
[16] W. Luo and U. Hengartner, *"Veriplace: A Privacy-Aware LocationProof Architecture,"* Proc. 18th SIGSPATIAL Int'l Conf. AdvancesGeographic Information Systems (GIS '10), Nov. 2010.
[17] 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.
[18] C. Ardagna, S. Jajodia, P. Samarati, and A. Stavrou, *"ProvidingMobile Users' Anonymity in Hybrid Networks,"* Proc. 15thEuropean Symp. Research Computer (ESORICS), Sept. 2010.
[19] 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.
[20] 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.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] M. Duckham and L. Kulik, *"A Formal Model of Obfuscation andNegotiation for Location Privacy,"* Proc. Int'l Conf. PervasiveComputing, May 2005.
[26] 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.
[27] 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.
[28] A. Beresford and F. Stajano, "*Location Privacy in PervasiveComputing,"* IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55,Jan.-Mar. 2003.
[29] 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.
[30] 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.
[31] J. Meyerowitz and R.R. Choudhury, *"Hiding Stars with Fireworks: Location Privacy through Camouflage,"* Proc. ACMMobiCom, Sept. 2009.
[32] www.yelp.com - Google Search. [Online]. Available: http://www.yelp.com/, 2012. [Accessed 5 November 2015].