# Location based rewarding system with security and privacy

Shailesh Dinde, Nilesh Mali, Vinod Kumbhar, Ashitosh Kharade, Ganesh Chinche, Akshay Kangle.

*Abstract*—***Promising as a new type of mobile marketing, mobile location-based services (MLBSs) have paying attention recently. The creation of mobile devices has motivated the mobile marketing to surge in the past few years. Unfortunately, current MLBSs have a lot of limitations and raise many concerns, especially about system security and users' privacy. In this paper, we propose a new location-based rewarding system, where mobile users can collect location-based tokens from token distributors, and then redeem their gathered tokens at token collectors for beneficial rewards. The token distributors and collectors can be any mercantile entities or that wish to catch the attention of customers through such a promotion system, such as stores, restaurants, etc. We develop location based rewarding system with security and privacy and prove the entirety and accuracy of the protocol. Moreover, we show that the system is flexible to various attacks and mobile users' privacy can be well protected. We finally create the system and conduct general experiments to validate the system effectiveness in terms of calculation, communication, power consumption, and storage costs.***

***Index Terms- Mobile location-based services, security, privacy.***

***Shailesh Dinde*, *Assistant Professor***, *Computer Science and engineering, Sanjay Ghodawat Institute, Atigre, India,*

***Nilesh Mali***, *Computer Science and engineering, Sanjay Ghodawat Institute, Atigre, Gadhinglaj, India, Mobile no.-8308110874*

***Vinod Kumbhar***, *Computer Science and engineering, Sanjay Ghodawat Institute, Atigre, Kothali, India. Mobile no.-7798857143*

***Ashitosh Kharade***, *Computer Science and engineering, Sanjay Ghodawat Institute, Atigre, Kumathe, India. Mobile no.-9766124876*

***Ganesh Chinche***, *Computer Science and engineering, Sanjay Ghodawat Institute, Atigre, . Latur, India. Mobile no.-9766820173*

## I. Introduction

Mobile marketing is an important issue in today world. Promising as a new type of mobile marketing, mobile location-based services (MLBSs) have paying attention recently. Mobile Location-based services (MLBS) applications that provide information to users based on their location are increasing business. From social networking to navigation to banking, consumers are being offered a range of new location-based services [2], [3]. Location based services are used in mobile apps also like book-my-show. Where, nearest cinema halls are showed to user. To know the relevant, timely and user engaging information and substance in mobile business knowledge of end user's mobile location is important thing in system.

System security and users' privacy is a main issues in existing Because mobile user mutually create location proofs and send updates to a location proof system. Each mobile device has its own pseudonyms which can be altered periodically to protect source.

A new type of MLBSs called location based check-in machinery system, which is based on location-based social networking, in which user can get favorable i.e. reward point in terms of rewards if they visit certain place again and again. In mobile location based marketing user can get certain rewards in form of reward points or money.

In this paper we propose privacy, secure and mobile location based rewarding system. The proposed system consists of trusted third party (TTP), token distributor (TD), token collector (TC), mobile user (MU) and central controller (CC). TTP issues certificate and verification with MU. TD issues tokens to MU. MU redeems all collected tokens at TC. The all information is stored at CC and at the time of redemption TC checks with CC.

In this system priority is given to security and privacy. We have made security about duplicate token redemption, colluding attack, impersonation attack, token tampering attack and multitoken request. Mobile user privacy is maintained in system.

## II. Previous work

Today there are many mobile location based services are present. In which some are based on e-commerce, some are related to location based service, some services are related to location based check-in system. Many users can lie about their location i.e. fake alibis by fixing on their locations and malicious users to access a restricted resource by knowing current location using location sensitive service. Zhichao Zhu explore A Privacy- Preserving Location proof Updating System (APPLAUS) in which the devices which are Bluetooth enable can automatically create their location proofs and renew in the system server. This created location proof is stored in user center server. One verifier is used to restrict and retrieve a location proof from server.

By using cellular base station user can get significant user location information, but problem is related to location history information which is not stored in system. For example 2G/3G system. Sun et al, utilize signal patterns to higher position users. They think about the multi-path signal patterns because the fingerprints of mobile devices, and approximate their locations by inspection received signals at a base location with those hold on in the information. Wanying Luo & Urs Hengartner According to Wanying et. al, user's location is the rough factor to facilitate the services. Authors have designed the everyplace: a location proof architecture, which enables users to collect the proof of being at proper location and enables the services to confirm these proofs.

Everyplace keep the network safe form the third party attacks and detects the cheating users who gather proofs for the places where they are not really located. User privacy is also key issue in location based system, users' privacy, with their information (e.g., identities and activities) and history. K anonymity cloaking schemes propose to cover a user's real location by incorporating its neighbors' location data. How ever, they need a secure trustworthy user-central server, would like the cooperation of a minimum of k neighboring users, and should sustain vital communication overhead. Another approach is location obfuscation. By adding noise to a user's real location, adversary cannot infer the user's real location from the user's location information. Obviously, this method is at the cost of service accuracy. Although using pseudonyms can protect users' privacy in onetime MLBSs, the server can continuously record users' unique-location information. Together all historical location information and particular side-information (e.g., working/living addresses) the adversary might be able to infer users' identities.

## III. Methodology

System consists of trusted third party(TTP), token distributor(TD), token collector(TC), mobile user(MU) and central controller(CC). The TTP issues certificate for the MU and verifies to respective MU. A mobile user then obtain token from token distributor. In this system MU can exchange them for acquiring rewards from not only from same store but also from any other retailers or brands.CC stores all information collected at TTP and TD and provide it to TC. TC collects token from MU.

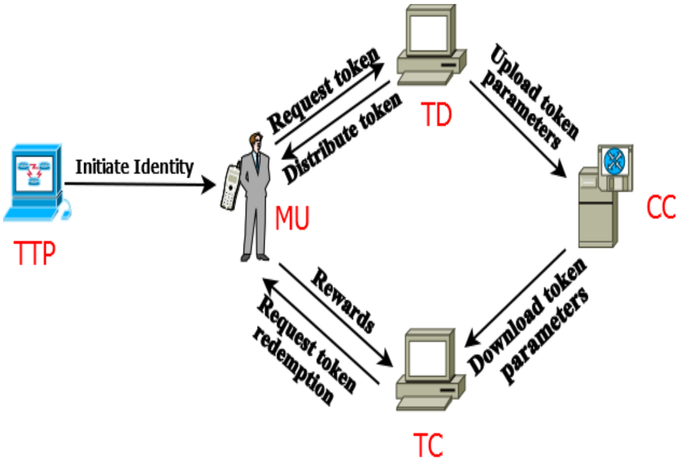

**Fig. System architecture**

**Trusted Third Party (TTP):** A trusted third party which gives each MU with an identity and certificate. The TTP is only responsible for issuing identities and not concerned in any other activities in the system.

**Mobile Users (MUs):** The mobile users which collect location-based tokens and redeem them for rewards. Each time that an MU visits a token distributor, it receives a token through its Wi-Fi network. Whenever an MU meets a token collector, it can redeem its collected tokens. After the token collector verifies that the tokens are redeemable, the MU will receive the corresponding rewards.

**Token Distributors (TDs):** The advertisement entities who issue redeemable tokens containing reward points to attract customers, such as shops, restaurants, etc. Each TD is equipped with a Wi-Fi access point (AP) which can allocate location-based tokens. Besides, each TD also generates corresponding audition information and stores it in the CC for future token verification.

**Token Collectors (TCs):** The advertisement entities who verify the MU's token redemptions and reward the MUs with benefits, for example, rewards, cash back, gifts. TCs communicate with MUs via Wi-Fi interfaces and are connected to the CC via the backbone network.

**Central Controller (CC):** As commonly used in many mobile application systems [4], [6], we consider an online Central Controller run by an independent third party. It is responsible for storing audition information of a token and forwarding it to a TC when asked to.

## IV. Design Goals

**System security:** completeness and soundness. Completeness means that MUs can always get tokens from TDs and redeem official tokens at TCs. Soundness refers to that the possibility that fake/duplicate tokens can be redeemed is neglected.

**User's privacy:** User's private information includes: first, MU's information like real identities, second, token information including the value of a token, and third, location histories. TCs are responsible for verifying MU's tokens to be redeemed, they cannot know MU's real identities, or any of the detailed token information except the values of the tokens to be redeemed, or MU's previous location histories.

## V. SECURITY AND PRIVACY ANALYSIS

### V.I Security Analysis

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

**Multi-token request attack:** When visiting a TD, a well behaved MU should get only one location-based token during each predefined time, while a misbehaving MU may generate fake token requests either by the same PID or by different PIDs, and try to get more than multitokens. By checking the existing request records in the time for duplicate PIDs or certi's, the TD can easily detect any multitoken request attack.

**Spare token redemption attack:** In the spare 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 Location based rewarding system. In particular, as mentioned before 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 the TC would check with the CC and can easily find out that this is a spare redemption.

**Impersonation attack:** An impersonation attack is that a misbehaving MU manages to steal another MU's tokens, in order to gain more rewards from a TC. Our system is also capable in defending against such misbehavior. In particular, in the first case, i.e., when a misbehaving MU uses another MU's PID and/or certi, to request for tokens, it cannot pass the identity authentication phase at the TD, since it does not know that MU's real identity. We have proven it in the soundness of the identity authentication phase.

**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 beneficial rewards. In the first case, since token is not obtained from a TD, there will not be any records at the CC. Thus, when the misbehaving MU tries to redeem the token at a TC, the TC can find out that there is no matching information for this token at the CC during the token audition phase and will terminate the redemption process.

**Colluding attack:** Colluding attack here refers to the misbehavior among MUs in the system trying to get illegal profit. In particular, in colluding attacks, some remote misbehaving MUs, who are not in the area of a TD, may try to get location-based tokens through some colluding MUs who are visiting the TD. It is assumed that MUs do not share their identities with each other [5], [9], due to the following reasons. First, an MU can impersonate another MU with that MU's real identity and hence get tokens and redeem tokens for benefits. Second, similar to that in [5], [10], [11], we can embed MU's identities in their mobile devices, for example, by using trusted computing components (TCCs) like trusted platform modules (TPMs) to store and bind their identities to the developed protocol.

### V.II Privacy Analysis

The privacy of MUs protected against other system entities, including, TDs, TCs, and the CC. A TD issues location-based tokens to MU's. So it has full knowledge of the tokens it has issued and knows the locations of those MUs when they visit it. However, since MUs only use their PIDs to request tokens, a TD cannot know the MU's real IDs, even though it can compare the certi's it has received tell if two requests are from the same MU. A TD cannot know the content of the tokens that MUs obtained from other TDs, or their location histories either. A TC collects location-based tokens and rewards the MUs with benefits. As described before, a TC only knows the value of the tokens it has accepted, but nothing else. It does not know the locations where these tokens were obtained, or the real IDs of the MUs redeeming the tokens. Besides, the same as TDs, a TC only knows the current location of some MUs when they visit it to redeem tokens and cannot know their location histories. In the case that TDs/TCs collude with other TDs/TCs, they basically exchange data regarding pidi's with the same certi and try to identify the MU. Since TDs/TCs do not know the real identities of any MUs in our system, even if some TDs/TCs collude with other TDs/TCs, they can only know the places, i.e., some TDs/TCs, which a certain anonymous MU has visited. Notice that in traditional location-based services, a user's queries may contain sensitive personal information, for example, habits, diseases, jobs, and more importantly, locations which could probably be his/her working place or home address.

Based on such history information, a location service server may be able to identify users with the help of some side information like their addresses [12], [13]. The locations recorded by the TDs/TCs are their own locations, which are all common public places. Therefore, the TDs/TCs will not be able to identify any MU even if they collude with each other.

The CC stores the audition information of the tokens issued by TDs. However, such information only contains MU's PIDs instead of their real IDs, and the tokens' audition parameters from which the CC cannot infer the content of the tokens.

### V.III Shared Symmetric Key

We employ the secret-splitting principle [7] to develop shared symmetric keys between MUs and TDs/TCs instead of using asymmetric keys. The reason is that when MUs use public/private key pairs, adversaries may be able to infer MU's identities by analyzing their public key patterns. In contrast, we use the following simple secret-splitting mechanism to generate a symmetric key between an MU and a TD or a TC: K1; 2 ¼ N1 XOR N2, where N1 and N2 are sufficiently large random numbers generated by the MU and the TD/TC, respectively.

## VI. Identity Initiation

Before an MU enters the system, it is issued by a TTP with a real identity si and a certificate certi of si.

When an MU, who is interested in collecting location-based tokens, visits TD, it initiates a token request conversation with this TD. The MU randomly generates a pseudonym (PID) based on its real identity (ID) to contact the TD, instead of directly using its real ID. Note that an MU updates its PID in each token request to avoid its real ID [34]. While on the TD's side, it first needs to check MU's identity before allocating a token. Thus, the token distribution process consists of two phases: MU's identity authentication and token distribution. Note that the MU's privacy should be protected during the whole process.

### MU's Identity Authentication at a TD

The purpose of authenticating an MU's identity before a TD distributes a location-based token is twofold. First, there might be misbehaving users who use fake IDs to generate PIDs in order to obtain more location-based tokens for more beneficial rewards. Second, identity authentication can efficiently defend against some of MU's misbehavior, for example, impersonation attack and colluding attack. In general, in the identity authentication phase, a TD checks if an MU has a valid ID without knowing the MU's real ID.

### Location-Based Token Distribution

If the MU can successfully pass the identity authentication phase, the TD would continue processing the MU's token request. In particular, the time window used by a TD is the duration within which each MU can only receive one location-based token from this TD.

The TD first checks if the token request is an excessive one by comparing i (obtained from certi) with the existing records within a specified time window. Since each MU only has one j corresponding to its identity as a test parameter, the TD can check the token request records, i.e., the MU's j's, in the current time window and see if there is already an existing record of i. If so, the TD determines the current token request is invalid, and does not issue a new token to the MU.

Finally, the TD generates audition information for this token. Since one of our objectives in system design is to keep the token's content as the MU's private information, the TD generates audition information and sends it instead of the token itself to the CC for future token verification at TCs.

There are mainly two reasons for generating audition parameters in such a way. First, since audition parameters contain full information of an issued token, it can be used for checking the integrity of a token. Second, the random number masked or hashed parameters prevent the CC from knowing the real content of the token, which might be compromised by adversaries.

### Token Redemption

Whenever an MU encounters a TC, it can redeem its collected location-based tokens by initiating a token redemption conversation with this TC. As we discussed above, the MU does not want to reveal its real identity or token information to the TC. On the other hand, the TC needs to make sure that this MU is a legal user, and that the token provided by the MU is intact and valid, and indeed belongs to itself, i.e., not stolen from someone else. Thus, the token redemption process is divided into four phases: MU's identity authentication, token audition, token property validation, and reward distribution. In the whole process, the user's privacy should be protected.

### MU's Identity Authentication at a TC

The TC first checks the MU's identity to make sure it is a legal user, for example, instead of an outsider adversary who tries to redeem a token stolen from some legal user. The phase of identity authentication at the TC is quite similar to the one at the TD, except a few changes Since the identity authentication phases at the TC and at the TD are the same, the completeness, soundness, and privacy reservation properties also hold at the TC.

## VII Token Audition

The purposes of token audition are: first, to make sure that the token submitted by the MU is valid and not generated by other entities than a TD, and second, to guarantee that the token is intact and has not been tampered since it was generated. On the other hand, since the token carries some private information of the MU, its content should be hidden from the TC. The basic idea is to let the TC only use the corresponding audition information retrieved from the CC to verify the token without knowing its content. In what follows, we describe the detailed token audition phase. Once the TC determines that this MU holds a valid ID which belongs to itself, it then uses this MU's PID, i.e., pidi contained in the token redemption request, to query for the corresponding token audition information from the CC.

### Token Property Validation

Even though the MU is a legal user who has a valid ID issued by the TTP, it might steal some legal users' tokens for redemption and can pass the previous two phases. Thus, the TC still needs to verify if the token belongs to this MU, which we call the token property validation phase. In particular, recall that the TC can retrieve the MU's certificate certi in the identity authentication phase. Otherwise, the token is not the MU's. The completeness, soundness, and privacy reservation of this phase can be easily proved, which are omitted here.

### Reward Distribution

After the MU trying to redeem a token passes the above three verification phases, the TC determines that this MU is qualified to redeem the token. Since in the previous verification phases, the MU's private information, including the value of this token v, is hidden from the TC, the MU needs to tell the TC v explicitly so that it can verify. For example, cash back or equivalent gift cards, to the MU. Otherwise, the TC aborts the redemption process. After the entire redemption process is finished, the TC informs the CC so that the CC just deletes this token permanently.

## VIII Conclusion

MLBS is mainly concern with privacy and security, in which it is important to maintain mobile user's location information private and secure. This system is mainly concerned with security and privacy. Security in terms of no third party can attack on system and redeems token. Privacy is maintained about mobile user. The information of mobile user is not shared with anyone and also their location also. We have created system with low storage costs, computation, communication and energy. Mobile Location Based services provide check-in system which provides beneficial rewards for MU those participate in system when mobile user visits commercial stores again.

## Reference

1. Ming Li, Sergio Salinas, and Pan Li, _LocaWard: A Security and Privacy Aware Location-Based Rewarding System_ IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL.25, NO. 2, FEBRUARY 2014.
2. W. Luo and U. Hengartner, "Proving Your Location Without Giving up Your Privacy," Proc. 11th Workshop Mobile Computing Systems Applications, Feb. 2010.
3. S. Saroiu and A. Wolman, "Enabling New Mobile Applications with Location Proofs," Proc. 10th Workshop Mobile Computing Systems Applications, Feb. 2009
4. Z. Zhu and G. Cao, "Towards Privacy Preserving and Collusion Resistance in Location Proof Updating System," IEEE Trans. Mobile Computing, vol. 12, no. 1, pp. 51-64, Nov. 2011.
5. W. Luo and U. Hengartner, "Veriplace: A Privacy-Aware Location Proof Architecture," Proc. 18th SIGSPATIAL Int'l Conf. Advances Geographic Information Systems (GIS '10), Nov. 2010.
6. R.A. Popa, A.J. Blumberg, H. Balakrishnan, and F.H. Li, "Privacy and Accountability for Location-Based Aggregate Statistics," Proc.18th ACM Conf. Computer Comm. Security, Oct. 2011.
7. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source
Code in C. Wiley, 1996.
8. C. Bettini, X.S. Wang, and S. Jajodia, "Protecting Privacy against Location-Based Personal Identification," Proc. Second VDLB Int'l Conf. Secure Data Management (SDM '05), Aug. 2005.
9. W. Luo and U. Hengartner, "Proving your Location without Giving up Your Privacy," Proc. ACM HotMobile, Feb. 2010.
10. M.S. Kirkpatrick and E. Bertino, "Enforcing Spatial Constraints for Mobile RBAC Systems," Proc. 15th ACM Symp. Access Control Models Technologies (SACMAT '10), June 2010.
11. M.S. Kirkpatrick, M.L. Damiani, and E. Bertino, "Prox-RBAC: A Proximity-Based Spatially Aware RBAC," Proc. 19th ACM SIGSPATIAL Int'l Conf. Advances Geographic Information Systems (GIS '11), Nov. 2011.
12. T. Xu and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-Based Services," Proc. IEEE INFOCOM, Apr. 2008.
13. M. Terrovitis and N. Mamoulis, "Privacy Preservation in the Publication of Trajectories," Proc. Ninth Int'l Conf. Mobile Data Management, Apr. 2008.