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

Mobile Based Marketing System Using Privacy and Security Aware Location Based Rewarding System

Digvijay A. Patil[1], Yogesh B. Gurav[2]

Professor, Savitribai Phule Pune University, PVPIT, Pune, India

Abstract: ***A Mobile location-based service (LBS) is a software application for a mobile device that requires knowledge about where the mobile device is located. Mobile location-based services use the geographic location of a personal handset – such as a personal digital assistant (PDA), smart phone or navigation device – either to enhance existing applications or to enable new applications. The consolidated utilization of wireless communication technology, location determination, geo-data frameworks and cell phones opens the best approach to create new or enhanced data, excitement, informal communication, individual route, mapping, geo-promoting, security, and law implementation following administrations, among others. Because of location sensitive system user can cheat about their current location and access restricted resources which will be harmful in mobile location based system. To preserve privacy and security, each mobile has pseudonyms are to protect source location privacy from each other which are periodically changeable with respect to specific condition and from the untrusted location proof server. In new proposed system mobile user can get identity and certificate from Trusted Third Party. Then mobile user can collect token from Token Distributor which will be act as virtual currency. And token collector can redeem the tokens from mobile user.***

Keywords: Mobile location-based services, security, privacy, Trusted Third Party, Mobile Users, Token Distributors, Token Collectors, Central Controller.

1. Introduction

Mobile marketing is an important issue in today world. Emerging as a new type of mobile marketing, mobile location-based services (MLBSs) have attracted intense attention recently. To know the relevant, timely and user engaging information and content in mobile commerce knowledge of end user's mobile location is important .If users with location-aware wireless devices can query about their surroundings for finding the nearest any place, anytime. MLBS offer tailored services that respond as you move from one place to another.

MLBS are isolated into eight administration classifications like mapping and route, neighborhood pursuit of mobile user and client data, interpersonal interaction and locator administrations, versatile asset administration, mobile advertising and marketing. Mobile clients represent an incredible test for the procurement of area based administrations to versatile clients.

System security and users' privacy is an important issue in current MLBS's because it has a lots of limitations with many concerns. Because mobile user mutually generate location proofs and send updates to a location proof server. Each mobile device has its own pseudonyms which can be changed periodically to protect source.

A new type of MLBSs called location based check-in technology system, which is based on location-based social networking, in which user can get beneficial 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 rewords in from of reword points or money. To completeness and soundness of the system a new system provides privacy and security.

2. Related Work

Although there have been several kinds of mobile location-based systems (MLBSs), including location based social networking [1], historical location proof services for some purposes [2]-[3], mobile commerce [4], and location-based check-in game , they cannot fully guarantee system security and user privacy.

First, for to acquire more benefits user can lie about their locations where they stay. This problem is very common in most MLBSs but has not been satisfactorily solved by existing system. Specifically, although cellular base stations may provide unforgeable real-time location information, the accuracy is not good enough and such location history information may not be available for use. For example, 2G/3G systems have localization accuracy of around 100 meters. Position estimation is based on static pictures, possibly provided by the mobile station. Where the position is determined in the network and presented to the user via a specific service are typically called network centric methods. This system has problem with in urban where the huge building are placed and indoor place in GPS positioning. This article does not cover low-layer issues related to the actual implementation of the wireless communication network. Of course, many important limitations on positioning can be found here. For instance, the resolution in AOA depends on antenna configuration. Timing measurements such as TOA and TDOA rely on synchronization and correlation techniques applied to known training sequences or pilot symbols. During line-of-sight (LOS), a rule of thumb is that timing can be achieved down to a fraction of the chip duration. Furthermore, non-line-of-sight (NLOS) causes information loss in all these measurements [5].

One possible solution to provide high-accuracy location information is to have Bluetooth enabled mobile Sun et al.

[6] utilize signal patterns to better position users. They consider the multi-path signal patterns as the "fingerprints" of mobile devices, and estimate their locations by comparing the received signals at a base station with those stored in the database. Anisetti et al. [7] explore Enhancements of mobile technologies are flooring the way to the definition of high-quality and accurate mobility prediction solutions based on data collected and managed by GSM/3G networks. To make it more Energetic and snappy than other positioning systems with respect to location spoofing and other terminal-based security threats , Geographic and mobility prediction both work at network and service level and Mobile network infrastructure is entirely same in whole system, and is entirely performed on the mobile network side, Our approach is based on a novel database correlation technique over Received Signal Strength Indication (RSSI) data, and provides a geographic and tracking technique based on advanced map- and mobility-based filtering. Above system explore geographic information and can achieve location accuracy of 65 meters with 95% correct rate.

Zhichao Zhu[8] explore A Privacy-Preserving Location proof Updating System (APPLAUS) which is used address the issues related to bogus alibis by cheating on their locations and malicious users to access a restricted resource by knowing current location using location – sensitive service. In which collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server.

Figure 1: Location proof updating architecture and message flow

Which are uploaded to a untrusted location proof server that can verify the trust level of each location proof. After that one authorized verifier is used to restrict or can query and retrieve location proof from the server. Each mobile device has statistically updated pseudonyms to protect from each other. Here user centric. User-centric location privacy model in which individual users evaluate their location privacy levels in real time and decide whether and when to accept a location proof request. mobile networks where mobile devices such as cellular phones communicate with each other through Bluetooth. In this system Mobile devices periodically initiate location proof requests to all neighboring devices through Bluetooth wireless network. After receiving a request, a mobile node decides whether to exchange location proof i.e location information, based on its own location proof updating requirement and its own privacy consideration.

Naveen Sastry, Umesh Shankar, David Wagner [9] have proposed echo protocol for secure in-region verification problem, which provides solution for the security issues in localization. In the network, identity with physical location of requester plays an important role for determining the access rights. Location verification enables location based access control to the requester and grant access to the resources based on the specified policy. To fulfill the proposed protocol is useful is secure and useful, its two properties- completeness and security are taken into consideration. Echo protocol has the verifier node, which sends packet with nonce(random value) to prover using the RF, and prover sends packet back to verifier node using ultrasound- to calculate the distance between each other, to assure that prover is in specific region or not. Authors have included innovative term- Region of Acceptance (ROA) in case of delay of the packet. It is the area in which verifier node is sure that it can correctly verify claim for the prover. For non circular region, ROA must be larger in scale that fits within the region. Echo protocol is used for location verification of the prover or the requester to communicate within particular region without cryptography. The proposed protocol is widely applicable in sensor networks, and the best suited for the cheap, small, mobile devices.

Wanying Luo & Urs Hengartner[10] According to Wanying et. al, user's location is the tough factor to enable the services. Authors have designed the Veriplace: a location proof architecture, which enables users to collect the proof of being at proper location and enables the services to validate these proofs. Veriplace keep the network safe form the third party attacks and detects the cheating users who collect proofs for the places where they are not actually located. It also preserves the user privacy. This architecture is implemented using the RSA with key length of 2048 bits and AES with key length of the 256 bits. The implementation of this architecture is rely on the PyCrypto's high performance library for implementation of the RSA for creating the signatures. The veriplace is designed for the 3 basic real-world services: service for the instructor to collect the class attendance, browser extension that adds location proof to emails, and the proof to the Yelp. Location proof daemon reads log configuration file on startup which contains the address of TTPL and TTPU, desired location granularity. Daemon send the location proof requests and saves the proof of the device. User can also request for the proof at once. Using the veriplace, authors have developed firefox extension to the Yelp app of iphone that lets reviewer attach the location proof to their reviews. Attached user proof is then retrieved from the location proof daemon to judge the proper location.

Second, an important part issues are users' privacy, it including user's personal data (e.g., identities and activities) and location information. Specifically, since the current systems use central servers to store all users' records, because of the use of central server they can easily know which users have ever been to which places at what times and for what purposes. This central storing server system puts users' privacy at risk. Unfortunately, users' privacy has been largely neglected current system design.

A few works propose schemes to achieve communication anonymity and data privacy in wireless networks, but are not applicable to MLBS scenarios. Although there have been

some works discussing users' location privacy, they all have their limitations. Wenbo He , Xue Liu y Hoang Nguyen , Klara Nahrstedt , Tarek Abdelzaher [11] explores, two schemes for providing privacy – preserving data aggregation Providing efficient data aggregation while preserving data privacy is a challenging problem in wireless sensor networks research. Cluster-based Private Data Aggregation (CPDA)– leverages clustering protocol and algebraic properties of polynomials. It has the advantage of incurring less communication overhead. The second scheme – Slice-Mix-AggRegaTe (SMART)– builds on slicing techniques and the associative property of addition. The main aim of this work is to bridge the gap between collaborative data collection by wireless sensor networks and data privacy.

Wensheng Zhang, Min Shao [12] explore, Data-Centric Sensor (DCS) networks for efficient data dissemination/access techniques and to find relevant data from within a sensor network, where the sensor data instead of sensor nodes are named based on attributes such as event type or geographic location. DCS explore the notion that the nature of the data is more important than the identities of the nodes that collect the data. Storing data inside a network also creates security problems due to the lack of tamper resistance of the sensor nodes and the unattended nature of the sensor network. To solve this problem pDCS is uest , pDCS means a privacy enhanced DCS network which offers different levels of data privacy based on different cryptographic keys.

k-anonymity cloaking schemes propose to hide a user's real location by incorporating its neighbors' location information. However, they require a secure trusted central server, need the cooperation of at least k neighboring users, and may incur significant communication overhead. Matt Duckham and Lars Kulik explore [13] obfuscation is an important technique for protecting an individual's location privacy within a pervasive computing environment. It has a framework within which obfuscated location-based services are defined. Claudio A. Ardagna, Marco Cremonini[14] explore different obfuscation operators to address different problem such as , when used individually or in combination in network, protect the privacy of the location information of users. they also explore guarantee different levels of location privacy to the users.

Aniket Pingley et. al.[15] has developed Context Aware Privacy Preserving (CAP) Location Based Service system to resolve the issues related to privacy protection in LBS. The key challenges of the problems - degree of privacy protection and LBS accuracy depends on the population and road density and another challenge is adversary may violate user's location privacy, considered in the implementation. CAP has Location Perturbing component perturb's the user's location and rearranges results returned by the LBS server, also CAP contains anonymous routing component which hides user's network identity. Designed system is focused on highly efficient terms of time and space complexity, rather than expensive services such as trusted third party-anonymizer. It improves the accuracy of LBS while taking communication QoS into account.

3. Design Modules and Architecture

In this section, we first present the architecture in Fig. 2, in which the system entities include Trusted Third Party (TTP), Mobile Users (MUs), Token Distributors (TDs), Token Collectors (TCs), and a Central Controller (CC). System consists of a trusted third party (TTP), mobile users (MUs), token distributors (TDs), token collectors (TCs), and a central controller (CC).

The TTP issues a corresponding certificate to each MU with a real identity. A legal mobile user can obtain a location-based token from Token distributor when mobile user visits commercial entity that participates in system. Token which are allocated to MU have different values but same can have same format. In this system MU can exchange them for acquiring rewards from not only at same store but also from any other retailers or brands. The amount of received rewards depends on the value represented by the collected tokens. Besides, the CC stores audition information of token sent by TDs and provide it to TCs when required.

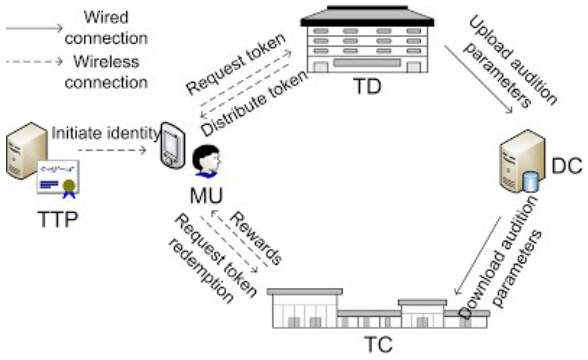

Figure 2: Architecture of system.

1) **Trusted Third Party (TTP):**
   To issues identity and a certificate for each mobile user (MU) A trusted third party works. The TTP is only responsible for issuing identities and not involved in any other activities in the system.
2) **Mobile Users (MUs):**
   The mobile devices which collect location-based tokens and redeem them for beneficial rewards. To collect token MU user visit token distributor and send request to token distributor and it receives token through WiFi. When MU user collects token it can be redeem that token to token collector by visiting TC. Token collector verifies that tokens are redeemable; the MU will receive the corresponding rewards. The communications between MUs and token collectors can also be carried out via their Wi-Fi interfaces.
3) **Token Distributors (TDs):**
   Token distributor used distribute token which are redeemable for getting beneficial rewards. The commercial entities such as stores, restaurants, and car rental companies who issue redeemable tokens containing reward points to attract customers. Wi-Fi access point is used as connection point for each TD to distribute location – based tokens. For future verification TD store corresponding information of mobile user in Central controller which is connected to TD by backbone wired network.

4) **Token Collectors (TCs):**
Token Collector works same as Token distributor for each mobile user. It collects token from Mobile user when any mobile user want to exchange their token and store audition information in central controller for further use.
5) **Central Controller (CC):**
Central controller play main role in check-in system. It store audition information related to mobile user who take part in system process. When any mobile user exchange their token TC first check, is the mobile user valid and then he check if visits that access point earlier or not using central controller. Actually Token distributor Token Collector and Central Controller works together for better system performances.

4. Conclusion

In this paper we try to analysis Mobile Location Based Services and improvement in system technology. MLBS is mainly concern with privacy and security, in which it is important to maintain mobile user's location information private and secure. For beneficial point mobile user in lie about their location information to acquire more detailed information. And MU can access restricted information also. So to avoid this problem there is need to be providing location proof for each Mobile user. And that location proof information also needs to be store in central controller for getting knowledge about valid user information. System uses trusted third party server to provide location proof to each mobile user i.e. Pseudonym which are periodically changes in the system. 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. For this purpose in this system each commercial store has Token Distributor and Token Collector. Which are used to distribute and collect the token.

Reference

[1] http://www.facebook.com/about/location.
[2] W. Luo and U. Hengartner, "Proving your location without giving up your privacy," in ACM HotMobile, Annapolis, Maryland, February 2010.
[3] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: Applications, challenges and implementations," in ACM Hot Mobile, Napa Valley, Califonia, February 2008.
[4] S. Loreto, T. Mecklin, M. Opsenica, and H.-M. Rissanen, "Service broker architecture: Location business case and mashups," IEEE Communication Magazine, vol. 47, no. 4, pp. 97–103, 2009.
[5] F. Gustafsson and F. Gunnarsson, "Mobile positioning using wireless networks," IEEE Signal Processing Magazine, vol. 22, no. 4,pp. 41–53, 2005.
[6] G. Sun, J. Chen, W. Guo, and K. R. Liu, "Signal processing techniques in network-aided positioning," IEEE Signal Processing Magzine, vol. 22, no. 4, pp. 12–23, 2005.
[7] M. Anisetti, C. A. Ardagna, V. Bellandi, E. Damiani, and S. Reale, "Map-based location and tracking in multipath outdoor mobile networks," IEEE Transactions on Wireless Communications, vol. 10, no. 3, pp. 814–824, 2011.
[8] Z. Zhu and G. Cao, "Towards privacy preserving and collusion resistance in location proof updating system," IEEE Transactions on Mobile Computing, vol. PP, no. 99, November 2011.
[9] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in ACM WiSE, San Diego, Califonia, September 2003.
[10] W. Luo and U. Hengartner, "Veriplace: A privacy-aware location proof architecture," in ACM GIS, San Jose, Maryland, ovember 2010.
[11] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "Pda: Privacy-preserving data aggregation in wireless sensor networks," in Proceedings of IEEE INFOCOM, Anchorage, Alaska,May 2007.
[12] M. Shao, S. Zhu, W. Zhang, and G. Cao, "pdcs: Security and privacy support for data-centric sensor networks," in Proceedings of IEEE INFOCOM, Anchorage, Alaska, May 2007.
[13] M. Gruteser and D. Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking," in ACM Mobisys'03, May 2003.
[14] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE Transactions on Mobile Computing, vol. 7, no. 1, pp. 1–18, January 2008.
[15] M. F.Mokbel, C. Y. Chow, andW. G. Aref, "The new casper: Query processing for location services without compromising privacy," in Proceedings of VLDB, 2006.
[16] Ming Lim,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