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

Mr. Digvijay A. Patil, Prof Yogesh B. Gurav

***Abstract*— A Mobile location-based service (MLBS) 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. 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. In today's location based system has number of limitation specifically related to preserve privacy and security. Proposed system is related to reward point allocation based on new check-in system. Where token acts as virtual money. Where clients can gather location area based tokens from token distributors, and after that reclaim their accumulated tokens at token collectors for getting prizes. Merchants wish to attract the customer so they provide number of offer to the customer i.e. nothing but reward points to the customer. To collect that extra reward points some malicious user can lie about their location, this is location cheating attack. To avoid this proposed system provides privacy and security to the user, each mobile has pseudonyms 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..**

Index Terms*— Mobile Marketing, Token Distribution, Location Based Service, Token Collection, Token Audition, Token Redemption

I. INTRODUCTION

Location Based Services is based on location related information. When you want to know nearest location information any restaurant or information of your one friend which in nearest area where you stay then location based service plays an important role [10], [13].

New emerging location based service is location based mobile marketing. In mobile marketing system if user location information then mobile commerce system can provide users requirement related information in time. Providing user engaging information is an important part in mobile commerce. In MLBS user apply a query to find nearest place of his requirement, then system provide efficient service as user moves from one place to another place. Mobile location based can be used for many purpose such location mapping, nearest user information, marketing and advertisement etc.

In mobile location based marketing system main issue is user privacy and user information security because of in this system is related with user location sensitive information, because of that if any user provide wrong information about their location then malicious user can access restricted resource as well as he can access private user information also. MLBS is also known as check-in system.

In proposed system check-in system is used. By using this system user can get reward point on their shopping. With privacy preserve location updating [3] feature for security of mobile user. In our system mobile user firstly gets certificate which can be known as licenses for system access and after that mobile user can participate in system process. Firstly mobile user sends a token request to the Token Distributor. Token Distributor then checks that mobile user is valid or not if it is valid then mobile user allow to get token and Token Distributor provides token to mobile user depends validation of user certificate. At the same time token distributor store mobile user information in the central controller for further use such as token redemption i.e. reward point allocation. Token redemption and reward point allocation is done by token collector. Reward point allocation is how many time users can visit to particular shop. For that purpose central controller check history of that mobile user based on its PID which generated by mobile user in Token Collector get it from the request which is send by mobile user.

II. RELATED WORK

Today's world there is several mobile location based services are available. 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. bogus alibis by cheating on their locations and malicious users to access a restricted resource by knowing current location using location sensitive service. Zhichao Zhu[3] explore A Privacy- Preserving Location proof Updating System (APPLAUS) in which the devices which are Bluetooth enable can manually generate their location proofs and update in the system server. This generated location proof is stored in user centric server. One verifier is used to restrict and retrieve a location proof from server. By using cellular base station user can get remarkable user location information, but problem is related to location history information which is not stored in system. For example 2G/3G system [4]. Sun et al. [5] utilize

Manuscript received June, 2015.

Mr. Digvijay A. Patil *, Computer Engineering,* Savitribai Phule University of Pune */PVPIT Bavdhan / Kolhapur,India,9860616635*

Prof. Yogesh B.Gurav*, Computer Engineering,* Savitribai Phule University of Pune */PVPIT Bavdhan. pune,india.*

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

signal patterns to higher position users. They think about the multi-path signal patterns because the "fingerprints" of mobile devices, and estimate their locations by examination the received signals at a base station with those hold on in the information. Wanying Luo & Urs Hengartner[6] According to Wanying et. al, user's location is the tough factor to enable the services. [7]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.

User privacy is also an important issue in location based system, users' privacy, together with their personal information (e.g., identities and activities) and site data, can be simply compromised. In the current system central server is used to store the user information which may cause problem when malicious user accesses the system. k-anonymity cloaking schemes [8]–[9] propose to cover a user's real location by incorporating its neighbors' location data. However, they need a secure trustworthy user-central server, would like the cooperation of a minimum of k neighboring users, and should incur vital communication overhead. Another approach is location obfuscation .By adding noise to a user's real location, adversary cannot infer the user's genuine location from the user's reported location information. Obviously, this method is at the cost of service accuracy. Besides, although using pseudonyms can protect users' privacy in onetime MLBSs, the server can continuously record users' pseudonym-location information. By piecing together all recorded historical location information and particular side-information (e.g., working/living addresses) [12] the adversary might be able to infer users' identities.

A. Review Stage

Submit your manuscript electronically for review.

III. System Architecture

As shown in system, Mobile User (MU) request for security certificate to the Trusted Third Party (TTP) server. Identification allocation and certificate creation has been done through the Trusted Third Party server. By using this certificate mobile user can request for tokens for marketing purpose to the Token Distributor (TD). Token Distributor verifies that certificate and if it is valid then Token Distributor allocate Token to the Mobile Users (MU). Using this allocated token user can buy any material from store in system. For this purposed Token Collector works, Token Collector exchange tokens by allocating some goods to that user. In this whole system , data collection and reward allocation is main thing which is done by the central controller , when user request for token – user data is store into the central controller for further use also when token collection is done then also token information and user information is store into the Central Controller. Central Controller counts how whether the user meet a store again and again depends upon that reward allocation is done. In mobile marketing system

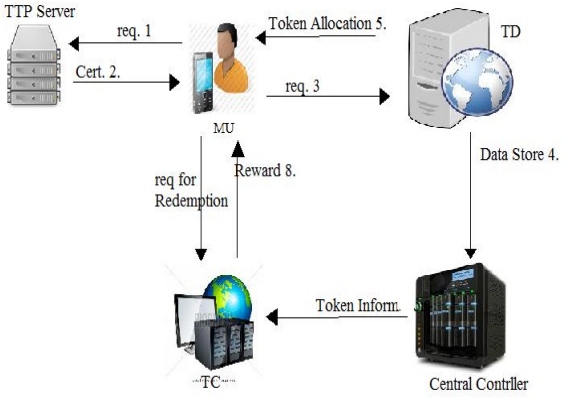


Fig. 1 *System Architecture*

which is based on location sensitive information of users. The Wi-Fi enabled system is required for this system. User with Certificate can become a part of the system. For secure transmission of the system shared symmetric key is generated between mobile user and token distributor and token collector.

IV. Preliminaries

A. Shared Symmetric Key

Symmetric Key encryption same key is used for data encryption and decryption. If no other party knows the key, then confidentiality is provided. No other party can recover the plaintext of the message. In this system for more security purpose shared symmetric key with key-splitting mechanism is used. For generating key k=N1 XOR N2 operation is used, N1 and N2 are two random number. This shared symmetric key is used in between MU and TD or TC. Actually shared symmetric key is used for to secure communication mobile user and token distributor as well as token allocator.

B. RSA Algorithm

For Identity initiation i.e. authority certificate generation RSA algorithm is used. As well as authentication purpose also RSA algorithm is used in our system. User firstly needs to registered, then trusted third party allocate real identity and certificate the user for further use. By using two random prime number p and q generate N_t which is actually product of p and q.

V. Set Theory

INPUT: Mobile user details and store details.
Let the system S is represented as:

S= {U,SD,C,T}
U be the user data
$U=\{U_{id}, U_{name}, U_{mail}, U_{mob}\}$
SD be the Store Data
$SD=(S_{id}, S_{name}, S_{brand})$
C be the Certificate Details
$C= (C_{id}, T_{cst}, R_{provg})$
T be the Token information
$T=\{T_{id}, TK_{cst}\}$

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

Mobile user register with system and for security reason system provides the trusted certificate to each mobile user and also provides token as money to each mobile user.

PROCESS: collect token from mobile user as per shopping (token collector collects token) and provides rewards points as per process to each mobile user (Token collector assigns rewards points)
$S = \{C_{gen}, C_{validate}, T_{assign}, R_{pt}\}$
C_{gen} be the Certificate Generation.
$F : \{ R_{prov}, P_{prov}, T_{cst}, U_{id}\} \rightarrow C_{gen}$
$C_{validate}$ be the certificate Verification.
$G : \{C_{id}, U, T_{cst}, P_{prov}\} \rightarrow C_{validate}$
T_{assign} be the Token Distribution
$FoG : \{C_{id}, T_{cst}, T_{id}\} \rightarrow T_{assign}$
R_{pt} be the reward points assignment.
$K : \{U_{id}, T_{cst}, C_{id}\} \rightarrow R_{pt}$
In the market mobile user moves to each store and connect their networks automatically, with verification of certificate assigned to mobile user through trusted third party and as per shopping redeem token and provides reward point to the user depends policy assign by store.

OUTPUT: Retrieve relevant data from server related to token and provide reward points.
Output = (Reward points data, Token collection data, Certificate report)
Mobile user give up the token in shop at the time of shopping then as per collected information and venders policy reward point are allocate to mobile user and each time verify the certificate and store the information in server

VI. System Modules

A. Certificate Creation and Allocation

To enter in the system, mobile user need to be having an authorized certificate $cert_i$ which is allocated by a trusted third party server with a real identity S_i. In this system for certificate creation RSA algorithm is used. RSA algorithm generates public key and private key for user, using this key information Trusted Third Party server generate certificate. For certificate creation, following algorithm is used.

Algorithm 1 Certificate Creation

Take two random prime numbers $p_t and q_t$
by using these calculate n_t
$n_t = p_t \times q_t$ where $p_t = 2kp_t' + 1$ and $q_t = 2kq_t' + 1$
TTP Chooses random integer e_i such that $1 < e_i < \phi(n_t)$
and $gcd(e_i, \phi(n_t)) = 1$ where
$\phi(n_t) = (p_t - 1)(q_t - 1)$;
Then $w^m = 1 mod n_t = w^{d_i} mod n_t$
public key $k_t^{pub} = \{e, n_t\}$
private key $k_t^{pri} = \{d_i, n_i\}$
Then computes value of $s_i = w^{d_i} mod n_t$
where $e_i d_i \equiv 1 mod \phi(n_t)^2$
by using private key , value of s_i
and value of $e_i d_i$ TTP generates certificate $cert_i$
$cert_i = M^{d_i} mod n_t$

Certificate generation algorithm that is been stated above uses any two prime number p_t and q_t then we use public key and private key of user for the generation of certificate. Here gcd is nothing but greatest common divisor. Value of e_i is assumed such that it should be in between 1 and value if $\phi(n_t)$ where n_t is nothing but product of assumed prime numbers.

B. Token Distribution

Mobile user those interested in token must visit to token distributor. Mobile user generate request to Token Distributor with it random PID. The real identity of mobile user must hide from process of token distribution as a measure for security of the user. On each request from Mobile User the system generates random PID. Token Distribution Process follows two phases: In the first phase authentication of Mobile user is done, the purpose of authentication is to restrict malicious user and to defend against MU's misbehavior. In this process Token Distributor verifies the mobile user i.e. its validation without checking its real ID. Mobile user send a request to TD distributor with its certificate. *cert i* ,

$$Req_D = k^{pub}_{TD} = (cert_i \| pid_i \| N_i)$$

where N_i is used of symmetric key generation. After request is received TD get an $cert_i$, N_i, pid_i of user through decryption user request by using its OWN private key k^{pri}_{TD}.. After receiving this whole information TD generate another random number N_d . *TD* generates shared session key using XOR operation of N_i and N_d . When session key generate TD distributor send N_d i.e. random key which is generated by TD. So by using this method data interchange between mobile user and token distributor is secure. In second phase, location based token distribution is involved. After certificate verification based on location and time window mobile user can get tokens. For this purpose first it checks the $cert_i$, then if is in certain time limit of the system then token distributor allocates token or generate new token using $cert_i$, pid_i , N_i , value of that token i.e. *v*.

C. Token Collection And Reward Point Allocation.

When any mobile user want to do shopping in system and if he/she has a location based tokens which are get form TTP then each mobile user meets particular token collector in the system. Here firstly conversation is happen in between mobile user and token collector. Token collector firstly checks that mobile user which wants to be a part of system is valid or not through certificate which is allocated to it. In token collection process is done through following process. In first process mobile user authentication at Token collector, this phase is somewhat similar to the process at TD authentication. In mobile marketing mobile user first send a request to the Token collector.

$$ReqD = k^{pub}_{TC}(cert_i \| pid_i \| N'_i)$$

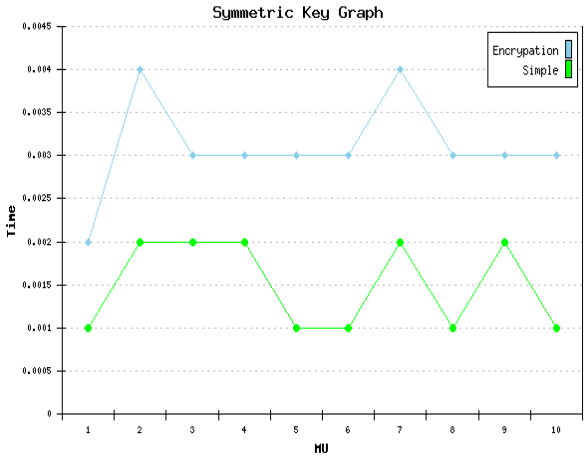
Here, N_i is random key generated for shared session key generation. *pid* obtained from token actually hides the real identity of user . This *pid* is pseudonym which are generated in particular manner. After that token audition process is done. In this process firstly token validation is checked whether the submitted token are valid or not i.e. it may be

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

submitted by other entities which are not the valid user. Secondly Token collector checks whether the submitted tokens are undamaged and not been tempered since they are generated. Token collector send query for Central Controller MU's audition information pid and shared symmetric key i.e. $K_{TC,CC}(pid)$. Then Central Controller performs duplicate redemption checking and sends back audition information to the TC. Last process is the Reward Point Allocation, which is depends upon the visiting count by any Mobile User to a particular store. In mobile marketing system if MU visits for particular store again and again then that store gives the reward points to that mobile user.

VII. Result Analysis

Result of the system in case of mobile is mostly concern with their computational time and computational cost and energy consumption in token distribution process.



In case of user communication in existing system and my proposed system, when user login with system, system checks the credentials like user name and password . But in existing system logins provides less security. Proposed system generates shared symmetric key. The key generated by this shared symmetric algorithm is again encrypted by Base64 algorithm. Half part of that key is stored at server and remaining half part at user site. So when user communicates with server, data encrypted with that symmetric keys and send towards server. So at the servers site, server can easily recognized where user is authorized or not. Communication cost graph shows communication delay during transaction. The time delay required for both the systems are nearly same but my proposed system provides more security with the same performance.

VIII. Conclusion

In this mobile marketing system, our additional module generates a new secure and privacy preserving system. Location based mobile marketing system is specifically based on location sensitive information. So user privacy is an important part in the system. Here we maintain user privacy by creating certificate and random PID for each process. We used check-in location based system which is useful for reward allocation marketing system. Because of secure verification and data transmission in the system computational time is less than other system as well computational cost is also low.

IX. Future Scope

Future work can involve in making check-in system for large communication area, with cloud technology or with any distributed computing technology.

Acknowledgment

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for making their guidance. We are thankful to the authorities of Savitribai Phule University of Pune. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

References

[1] 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, FEBRUARY2014.

[2] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proceedings of IEEE ICDCS*, Columbus, Ohio, June 2005.

[3] 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.

[4] F. Gustafsson and F. Gunnarsson, "Mobile positioning using wireless networks," *IEEE Signal Processing Magzine*, vol. 22, no. 4, pp. 41–53, 2005.

[5] 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.

[6] 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

[7] 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

[8] M. Gruteser and D. Grunwald, "Anonymous usage of locationbased services through spatial and temporal cloaking," in *ACM Mobisys'03*, May 2003.

[9] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 12, pp. 1719 – 1733, December 2007.

[10] http://www.facebook.com/about/location

[11] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *ACM WiSE*, San Diego, Califonia, September 2003.

[12] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proceedings of IEEE ICPS*, Santorini, Greece, July 2006.

[13] https://foursquare.com/

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET