

# A Secure Location-Based Coupon Redeeming System

J. Maruthi Nagendra Prasad and A. Subramanyam

**Abstract** With the rapid evolution of mobile computing technologies, Mobile location based services are identified as one of the most promising target application. Mobile location based services have lot of limiting factors. In this paper we propose a new rewarding system based on location of the Mobile User where Mobile Units will collect Coupons from the Coupon Distribution Center and then redeem their Coupon's at the Coupon Collection Center. Coupons acts as virtual currency Coupon's Distributers and Collectors can be any entity or retailer. This rewarding system based on location of the Mobile Unit is a secure one and preserves privacy of the Mobile user.

**Keywords** Mobile location based services • Rewards • Coupons • Privacy • Security

## 1 Introduction

With the proliferation of mobile devices, mobile location-based services (MLBSs) have emerged as a new type of mobile marketing. Mobile commerce is poised to make a qualitative leap. Knowledge of the end user's location will be used to deliver relevant, timely, and engaging content and information. For mobile network operators, location-based services represent an additional stream of revenue that can be generated from their investments in fixed infrastructure. For the end user, these services can help reduce confusion, improve the consumption experience, and deliver high-quality service options. As per a report 1 % of Americans used MLBSs [1]. Research conducted by Juniper predict that revenue generated by MLBS's will be more than \$12.7 billion by 2014 [2].

---

J. Maruthi Nagendra Prasad (✉) • A. Subramanyam  
AITS, Rajampet, India  
e-mail: maruthiprasad1986@gmail.com

A. Subramanyam  
e-mail: smarige@gmail.com

There are various kinds of Mobile Location Based Services. First one is social networking based on Location [3]. Second one require users to provide current or historical location proofs to fulfill some purposes [4]. Third one is Mobile Commerce [5] and Fourth one is check-in games based on location [6].

Location-based check in games are having 3 restrictions first mobile users can get benefits from the same store, second security is not guaranteed in this system [7, 8] and third is preserving users privacy is difficult.

Here, we propose a rewarding system based on mobile location. The proposed system consists of a Mobile Unit, Coupon Distribution Center, Coupon Collection Center, Data Center and Authentication Center. Mobile Unit will collect Coupon's from the Coupon Distribution Center and Mobile Unit can redeem the Coupons for rewards at the Coupon Collection Center. Data Center stores the Mobile Unit and Coupon validation details, used to validate the Coupon before rewarding the Mobile User. Data Center is used when Coupon Distribution Center and Coupon Collection Center happens to be of the same retailer.

If the Coupon Distribution Center and Coupon Collection Center are from different retailer instead of Data Center Authentication Center is used which validate the Mobile User and Coupon. Communication between MU and CDC/CCC carried out via WiFi interface. CDC/CCC are connected to the DC through wired network.

## 2 Related Work

In spite of the fact that there are many flavors of Mobile Location based systems they cannot ensure security of the system and privacy for the users.

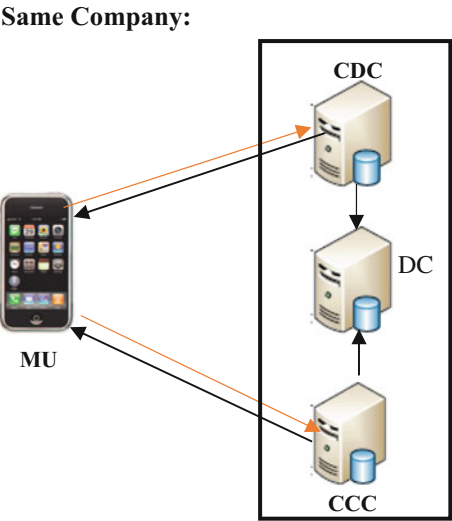
First users can fake their location to get more benefits, this problem can be addressed by sun et al. [9] uses signal patterns to position users. Anisetti et al. [10] explore geographical information and can achieve location accuracy and using Bluetooth for generating location proofs [11]. Lenders et al. [12] uses geo-tags. [13, 8] propose to use Wi-Fi.

Second User's Privacy can be compromised. [14–20] Propose schemes to achieve communication anonymity and data privacy k-anonymity Clocking scheme [15–19], propose to hide real location of the user and others include obfuscation of location [20], and using pseudonyms.

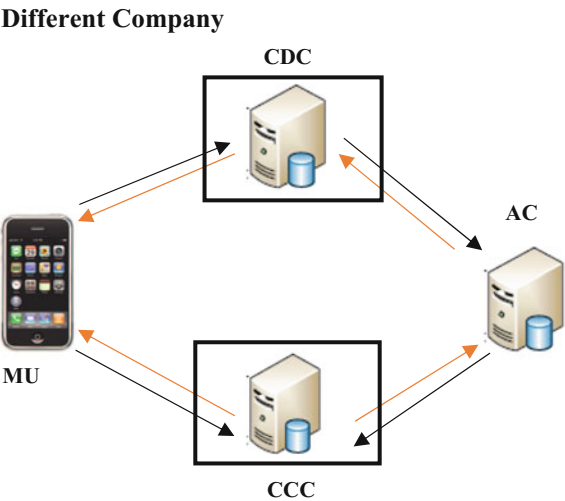
## 3 System Design

This system consists of Mobile User's (MU), Coupon Distribution Center (CDC), Coupon Collection Center (CCC) and Data Center (DC) or Authentication Center (AC) as shown in Figs. 1 and 2.

**Fig. 1** Same Company Scenario where CDC and CCC belongs to same company or retailer



**Fig. 2** Different Company scenario where CDC and CCC belongs to the different retailers



**Mobile Users (MUs):** A Mobile Unit collects the coupons and redeem for rewards. For collecting coupons Mobile User communicates with Coupon Distribution Center and redeems the Coupon when it communicates with Coupon Collection Center.

**Coupon Distribution Center (CDC):** Coupon Distribution Center generates the Coupon for the Mobile Unit and Stores the Mobile User validation information and coupon information in the Data Center or in Authentication Center.

**Data Center or Authentication Center:** it validates the Mobile User and coupon.

**Table 1** Shared secret keys in the Rewarding system based on the location of the mobile user

Shared secret key	Purpose
K d, c	Shared secret key between CDC and CCC
K i, d	Shared secret key between MU and CDC
K i, c	Shared secret key between MU and CCC
K d, dc	Shared secret key between CDC and DC
K c, dc	Shared secret key between CCC and DC
K d, a	Shared secret key between CDC and AC
K c, a	Shared secret key between CCC and AC

**Coupon Collection Center (CCC):** This entity verify the Mobile User' coupon and rewards them with benefits.

#### Shared Secret Key Generation:

As Assume two mobile users user1 and user2 either one of them pick large prime numbers  $n$  and  $g$ . User1 picks a large number  $x$  and keep it secret and User2 picks a large number  $y$  and keep it secret User1 initiates the key exchange protocol by sending User2 a message containing  $(n, g, g^x \bmod n)$ .

User2 responds by sending User1 a message containing  $g^y \bmod n$ . Now User1 computes  $(g^y \bmod n)^x \bmod n = g^{xy} \bmod n$ . Similarly User2 computes  $(g^x \bmod n)^y \bmod n = g^{xy} \bmod n$ , in the similar fashion shared secret keys shown in Table 1 can be generated.

## 4 Rewarding System

As Here the system consists of following processes:

#### Coupon Distribution:

Whenever a Mobile User visits a CDC it requests a Coupon. To protect identity of the Mobile User and preserve the location details MU randomly generates a pseudonym based on real identity. CDC needs to check MU's identity before allocating a coupon.

#### Thus CDC consists of two phases

- MU's Identity authentication:  
Purpose of validating an MU's identity is defend against misbehaving users who use fake ids.
- Coupon Distribution:  
If the MU completes the identity authentication the CDC will process the MU's token.

**Coupon Redemption:**

Whenever an MU communicates with CCC it initiates a token redemption process.

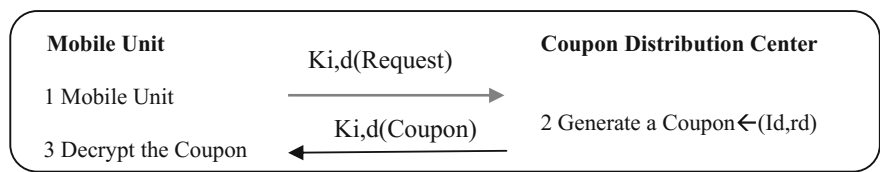
**Thus CCC consists of three phases:**

- **MU’s Identity Authentication at CCC:**  
CCC first checks the MU’s identity to make sure it’s an authorized user and this phase is similar to MU’s Identity authentication in CDC.
- **Coupon validation:**  
This phase is used to validate the coupon submitted.
- **Reward Distribution:**  
After the MU and coupon validation completes then benefits will be rewarded to the MU.

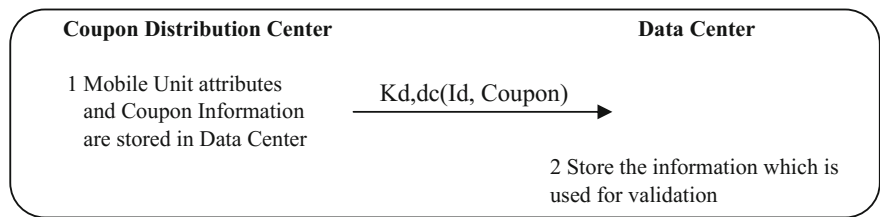
Rewarding system based on Location of the Mobile User includes the following steps:

**Sample Scenario:**

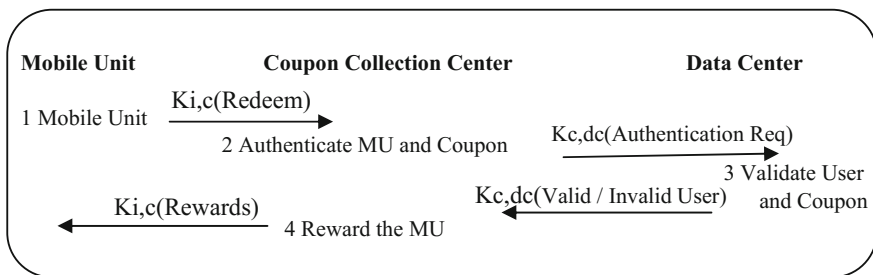
See (Figs. 3, 4, and 5)



**Fig. 3** Shows interaction between Mobile Unit and CDC using shared secret key  $K_{i,d}$  where generated coupon will be consisting of Id of the MU and a random number



**Fig. 4** Shows interaction between CDC and DC using shared secret key  $K_{d,dc}$



**Fig. 5** Shows interaction between MU and CCC and DC using the shared secret keys  $K_i, c$  and  $K_c, dc$

## 5 Conclusion

Here we proposed a secure and privacy preserving rewarding system based on location of the mobile user. We designed secured and privacy aware system for redeeming the rewards. We find the system is resilient to many attacks and privacy of the mobile unit will be protected well.

## References

1. <http://pewinternet.org/~media/Files/Reports/2010/PIP-location%20based%20services.pdf> (2010)
2. Juniper Research, Mobile Location Based Services Applications, Forecasts and Opportunities 2010–2014
3. <http://www.facebook.com/about/location>
4. Lenders V, Koukoumidis E, Zhang P, Martonosi M (2008) Location-based trust for mobile user-generated content: applications, challenges and implementations. In: Proceedings of the ninth workshop mobile computing systems applications (HotMobile'08)
5. Loreto S, Mecklin T, Opsenica M, Rissanen H-M (2009) Service broker architecture: location business case and mashups. *IEEE Comm Mag* 47(4):97–103
6. <https://foursquare.com/>
7. Sastry N, Shankar U, Wagner D (2003) Secure verification of location claims. In: Proceedings of the second ACM workshop wireless security (WiSe'03)
8. Luo W, Hengartner U (2010) Veriplace: a privacy-aware location proof architecture. In: Proceedings of the 18th SIGSPATIAL international conference advances geographic information systems (GIS'10)
9. Sun G, Chen J, Guo W, Liu KR (2005) Signal processing techniques in network-aided positioning. *IEEE Signal Process Mag* 22(4):12–23
10. Anisetti M, Ardagna CA, Bellandi V, Damiani E, Reale S (2011) Map-based location and tracking in multipath outdoor mobile networks. *IEEE Trans Wireless Commun* 10(3):814–824
11. Zhu Z, Cao G (2011) Towards privacy preserving and collusion resistance in location proof updating system. *IEEE Trans Mobile Comput* 99
12. Lenders V, Koukoumidis E, Zhang P, Martonosi M (2008) Location-based trust for mobile user-generated content: applications, challenges and implementations. In: ACM HotMobile, Napa Valley, California

13. Saroiu S, Wolman A (2009) Enabling new mobile applications with location proofs. In: ACM HotMobile, Santa Cruz, California
14. Kong J, Hong X (2003) Anodr: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In: Proceeding of ACM MobiHoc, Annapolis, Maryland
15. Gruteser M, Grunwald D (2003) anonymous usage of location-based services through spatial and temporal cloaking. In: proceedings of the first international conference mobile systems, applications services (Mobisys'03)
16. Gedik B, Liu L (2008) Protecting location privacy with personalized K-anonymity: architecture and algorithms. IEEE Trans Mobile Comput 7(1):1–18
17. Kalnis P, Ghinita G, Mouratidis K, Papadias D (2007) Preventing location-based identity inference in anonymous spatial queries. IEEE Trans Knowl Data Eng 19(12):1719–1733
18. Gedik B, Liu L (2005) Location privacy in mobile systems: a personalized anonymization model. In: Proceedings of the IEEE 25th international conference distributed computing systems (ICDCS)
19. Kido H, Yanagisawa Y, Satoh T (2006) An anonymous communication technique using dummies for location-based services. In: Proceedings of the IEEE 25th international conference distributed computing systems (ICDCS)
20. Ardagna C, Jajodia S, Samarati P, Stavrou A (2010) Providing mobile users' anonymity in hybrid networks. In: Proceedings of the 15th European symposium on research in computer security (ESORICS), Athens, Greece

Emerging Trends in Electrical, Communications and  
Information Technologies

Proceedings of ICECIT-2015

Attele, K.R.; Kumar, A.; Sankar, V.; Rao, N.V.; Hitendra  
Sarma, T. (Eds.)

2017, XIII, 458 p. 233 illus., Hardcover

ISBN: 978-981-10-1538-0