LOCAWARD: A SECURITY AND PRIVACY AWARE LOCATION-BASED REWARDING SYSTEM

Madhuri Martis[1], Rameshkumar H K[2]

[1]M.Tech Student, [2]Assistant Professor, Dept. of Computer Science and Engineering,
STJIT, Ranebennur, Karnataka, (India)

ABSTRACT

The proliferation of mobile devices has driven the mobile marketing to surge in the past few years. Emerging as a new type of mobile marketing, mobile location-based services (MLBS's) have attracted intense attention recently. Unfortunately, current MLBS's have a lot of limitations and raise many concerns, especially about system security and user's privacy. We propose a new location-based rewarding system, called LocaWard, where mobile users can collect location-based tokens from token distributors, and then redeem their gathered tokens at token collectors for beneficial rewards. Tokens act as virtual currency. The token distributors and collectors can be any commercial entities or merchants that wish to attract customers through such a promotion system, such as stores, restaurants, and car rental companies. We develop a security and privacy aware location-based rewarding protocol for the LocaWard system, and prove the completeness and soundness of the protocol. Moreover, we show that the system is resilient to various attacks and mobile users' privacy can be well protected in the meantime. We finally implement the system and conduct extensive experiments to validate the system efficiency in terms of computation, communication, energy consumption, and storage costs.

Keywords: Trusted Third Party (TTP), Mobile User's (MU''s), Central Controller (CC), Token Collectors (TC's), Token Distributors (TD's.

I. INTRODUCTION

With the rapid evolution of mobile devices, mobile location-based services (MLBSs) have emerged as a new type of mobile marketing. According to a 2010 report by Pew Research Center, on any given day, 1 per cent of online Americans used MLBSs. Juniper Research predicts that the revenues from MLBSs will surge to more than $12.7 billion by 2014.

Currently, there are various kinds of MLBSs. One of them is location-based social networking, such as Facebook Places, where users share their locations with friends and find others who are nearby. Another type of MLBSs requires the users to provide current or historical location proof to fulfil some purposes. For example, a hospital may allow doctors or nurses to access patients' documents only when they can prove that they are in a particular room of the hospital. A person accused of committing a crime is very much interested in being able to prove to the police that he was somewhere else rather than at the crime scene while the crime was committed. '

Mobile commerce is another branch of MLBS's, for example, forwarding advertisements to customers when they are near a business spot. These MLBS's do not consider rewarding services.

More recently, a new type of MLBS's called location based check-in game, which is developed based on location-based social networking, lets users earn beneficial rewards if they visit certain places. In particular, some applications, including Foursquare, and Loopt Star let users check in different locales (e.g., coffee shops, restaurants, shopping malls) to not only compete with friends in games, but also earn rewards, points, or discounts from retailers and organizations.

The rewards and reward amounts can be different depending on time of day, how frequently the person has checked it in the past, and so on. However, these location-based check-in systems are limited in several aspects.

II. BACKGROUND

In particular, since the current systems use central servers to store all users' records, they can easily know which users have ever been to which places at what times for what purposes. Previous works on users' identity privacy in wireless networks are not applicable to MLB's .Figure. 1 shows the existing scenario

Although there has been some research on location privacy regarding general location-based services, such as k-anonymity cloaking, location obfuscation, pseudonym exchanges in mix zones, they all have their limitations

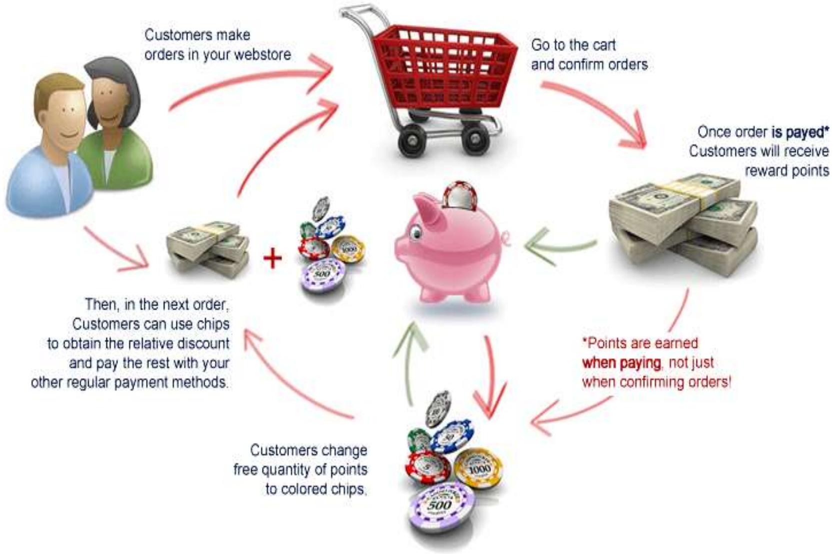

Figure 1: Existing System

III. RELATED WORK

Here we propose a secure, privacy-preserving, and realistic mobile location-based rewarding system, called LocaWard, which strives to address the above concerns. The proposed system consists of a trusted third party (TTP), mobile users (MU's), token distributors (TD's), token collectors (TC's), and a central controller (CC). The TTP issues each MU with a real identity and a corresponding certificate.

IV. SCOPE OF THE PROJECT

We will propose a secure, privacy preserving, and realistic location-based rewarding system, LocaWard. We will design a security and privacy aware protocol for the LocaWard system and prove its completeness and soundness.

We find that the system is resilient to many types of attacks and mobile user's privacy can be well protected as well. We will also evaluate the system efficiency by extensive real experiments and show that the computation, communication, energy, and storage costs are low.

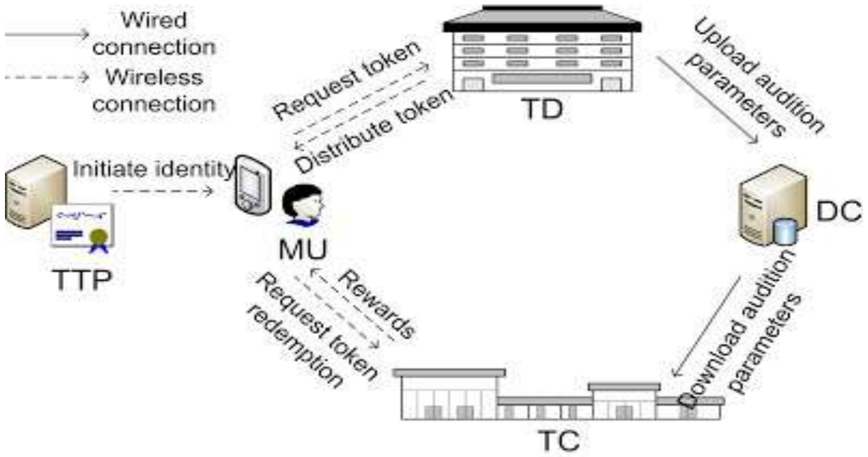

Figure 2: System Architecture

In LocaWard, the system entities include a Trusted Third Party (TTP), Mobile Users (MU's), Token Distributors (TD's), Token Collectors (TC's), and a Central Controller (CC). In what follows, we describe the functionalities and interactions of these system entities. Trusted Third Party (TTP): A trusted third party which issues each MU with an identity and a certificate. The TTP is only responsible for issuing identities and not involved in any other activities in the system.

4.1 Mobile Users (MU's)

The mobile devices which collect location-based tokens and redeem them for beneficial rewards. Each time that an MU visits a token distributor, it sends a request and receives a token through its WiFi interface. Whenever an MU meets a token collector, it can redeem its gathered tokens. After the token collector verifies that the tokens are redeemable, the MU will receive the corresponding rewards. The communications between MU's and token collectors can also be carried out via their Wi-Fi interfaces.

4.2 Token Distributors (TD's)

The commercial entities who issue redeemable tokens containing reward points to attract customers, such as stores, restaurants, and car rental companies. Each TD is equipped with a WiFi access point (AP) which can distribute location-based tokens. Besides, each TD also generates corresponding audition information and stores it in the CC for future token verification. TDs are connected to the CC through a backbone wired network, say the Internet.

4.3 Token Collectors (TCs)

The commercial entities who verify the MUs' token redemptions and reward the MUs

with benefits, for example, monetary rewards, coupons, gift cards. TCs communicate with MUs via WiFi interfaces and are connected to the CC via the backbone network. Note that some TDs can serve as TCs at the same time.

4.4 Central Controller (CC)

As commonly used in many mobile application systems we consider an online Center 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.

V. PROPOSED METHODOLOGY

Here we propose a secure, privacy preserving, and realistic mobile location based rewarding system, called LocaWard, which strives to address the above concerns. The proposed 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 each MU with a real identity and a corresponding certificate. A legal MU is able to obtain a location based token when it visits a commercial entity that participates in the system, i.e., a TD.

The issued tokens at various TDs have the same format but possibly different indicated values. With all the collected tokens, an MU can redeem them for beneficial rewards not only at the same store or brand stores, but also at any other retailers or commercial entities, i.e., TCs, that have joined the system.

The amount of received rewards depends on the value represented by the collected tokens. Besides, the CC stores token audition information sent by TDs and provides it to TCs when required. Then, we design a security and privacy aware location based rewarding protocol for the proposed LocaWard system.

We assume that TDs, TCs, and the CC work in the semi honest mode, i.e., they faithfully and correctly execute the system protocol but are curious about MUs' privacy, including their personal information like real identities, token information, and location histories. Specifically, the protocol is composed of three parts: identity initiation, token distribution, and token redemption. In identity initiation, the TTP issues each MU with an identity and a corresponding certificate. Each MU keeps its identity private and generates a new pseudonym for each token request or redemption. The certificate is used for a user's identity authentication without revealing its real identity. In token distribution, a TD needs to verify if an MU requesting a token is a legal user in the system without knowing its real ID. After that, the TD issues the MU with an anonymous token which can be redeemed at any TC for rewards.

VI. CONCLUSION

Here we have proposed a secure, privacy preserving, and realistic location-based rewarding system, LocaWard. We have designed a security and privacy aware protocol for the LocaWard system and proven its completeness and soundness. We find that the system is resilient to many types of attacks and mobile users' privacy can be well protected as well.

We have also evaluated the system efficiency by extensive real experiments and show that the computation, communication, energy, and storage costs are low. Moreover, although the proposed security and privacy aware location-based rewarding protocol is for our LocaWard system, the techniques herein can be generalized to address security and privacy problems in general location based services and other areas like cloud computing.

VII. ACKNOWLEDGEMENT

I consider it is a privilege to express my gratitude and respect to all those who guiding me in the progress of my paper.

I wish my grateful thanks to Mr. Rameshkumar H K M.Tech, project guide, for his invaluable support and guidance. Madhuri Martis

REFERENCES

[1] Juniper Research, Mobile Location Based Services Applications, Forecasts and Opportunities 2010-2014, https://www. juniperre-search.com/reports/mobile_location_based_services, 2010.

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

[3] W. Luo and U. Hengartner, "Proving Your Location Without Giving up Your Privacy," Proc. 11th Workshop Mobile Computing Systems Applications, Feb. 2010.

[4] S. Saroiu and A. Wolman, "Enabling New Mobile Applications with Location Proofs," Proc. 10th Workshop Mobile Computing Systems Applications, Feb. 2009.

[5] 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.

[6] S. Loreto, T. Mecklin, M. Opsenica, and H.-M. Rissanen, "Service Broker Architecture: Location Business Case and Mashups," IEEE Comm. Magazine, vol. 47, no. 4, pp. 97-103, Apr. 2009.

[7] https://foursquare.com/.

[8] "JPBC: Java Pairing Based Cryptography," http://gas.dia.unisa. it/projects/jpbc.

BIOGRAPHY

Madhuri Martis is a student pursuing her Master degree in Computer Science and Engineering department at STJ Institute of Technology, Ranebennur, Karnataka, India. Her research interests are Computer Science related aspects such as Networking technology, Java programming language and web 2.0.

Ramesh kumar H K, is assistant professor in the department of Computer Science and Engineering at STJ Institute of Technology, Ranebennur, Karnataka, India. He received his Master degree in Computer Networks. His research interests are related to computer networks.

.