Local Ward A Security and Privacy Aware Location-Based Rewarding System

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 (MLBSs) have attracted intense attention recently. 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, 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.
EXISTING SYSTEM:

The location-based social networking is a type of MLBS, 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 fulfill some purposes. Mobile commerce is another branch of MLBSs.

There is a new type of MLBSs called location-based check-in game, which is developed based on location-based social networking, letting 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.

PROBLEM DEFINITION:

- Customers can only receive and redeem rewards at the same brand stores or even the same store only. This greatly weakens the customers’ motivations for visiting the locales.
From a service provider’s perspective, security is not guaranteed in the existing systems. Since users can receive benefits for visiting some places, they have incentives to claim that they are at certain locations even though they are not. Most of those location-based check-in applications (e.g., Foursquare) use the GPS on a user’s mobile device to verify the location claimed by the user. However, users may cheat on their locations.

Third, from users’ perspective, users’ privacy including identity privacy and location privacy has been largely ignored in the current check-in systems. 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.

PROPOSED SYSTEM:

- 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.

- We design a security and privacy aware location based rewarding protocol for the proposed LocaWard system. The protocol is composed of three parts: identity initiation, token distribution, and token redemption.

ADVANTAGES OF PROPOSED SYSTEM:

- System security: Completeness and soundness. Completeness means that honest MUs can always successfully obtain tokens from TDs and redeem valid tokens at TCs. Soundness refers to that the probability that forged/tampered/stolen tokens can be redeemed is negligible.

- Users’ privacy: Users’ private information includes: MUs’ personal information like real identities, token information including the value of a token, and location histories

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
IEEE Projects 100% WORKING CODE + DOCUMENTATION + EXPLANATION – BEST PRICE
LOW PRICE GUARANTEED

- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : Windows XP/7.
- Coding Language : JAVA/J2EE
- IDE : Netbeans 7.4
- Database : MYSQL