Pervasive and Mobile Computing 49 (2018) 139–152

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Privacy-respecting reward generation and accumulation for participatory sensing applications

Tassos Dimitriou

Computer Engineering Department, Kuwait University, Kuwait

ARTICLE INFO

Article history:
Received 20 October 2017
Received in revised form 9 April 2018
Accepted 9 July 2018
Available online xxxx

Keywords:
Rewards
Incentives
User privacy
Anonymity
Credential systems
Zero-knowledge proofs
Participatory sensing
Crowd sensing

ABSTRACT

Participatory or crowd-sensing applications process sensory data contributed by users and transform them to simple visualizations (such as for example noise or pollution levels) that help create an accurate representation of the surrounding environment. Although contributed data is of great interest to individuals, the involvement of citizens and community groups, however, is still limited. Thus, incentivizing users to increase participation seems crucial for the success of participatory sensing.

In this paper, we develop a privacy-preserving rewarding scheme which allows campaign administrators to reward users for the data they contribute. Our system of anonymous tokens allow users to enjoy the benefits of participation while at the same time ensuring their anonymity. Moreover, rewards can be accumulated together thus further increasing the level of privacy offered by the system. Our proposal is coupled with a security analysis showing the privacy-preserving character of the system along with an efficiency analysis demonstrating the feasibility of our approach in realistic deployment settings.

1. Introduction

Participatory sensing (or crowd-sensing) is a new paradigm for data collection and knowledge representation that has been enabled by the proliferation of mobile devices with sensing capabilities. Using the sensors embedded in smart phones and other similar devices, users can interact with the environment and create a better understanding of people's activities and their surroundings. Participatory sensing applications are numerous; participants can monitor and report environmental conditions such as noise or air pollution, they can document health related issues or physical activities, they can monitor road and traffic conditions, and so on [1].

The key factor for the success of crowd-sensing applications is user participation. Even though the use of smart phones and tablets has made participation easy, voluntary commitment of participants is still limited. This is mostly due to the fact that users do not see any immediate benefits for contributing the sensing capabilities of their mobile devices. Thus incentivizing users to increase the amount and the quality of the data they submit seems necessary for the success of participatory sensing applications.

An important research direction in this area has been to come up with the right incentives that would make people more involved in the data collection process. This is typically done by defining appropriate mechanisms which can be used to reward users for their sensed data while at the same time maximizing the utility of the collected data. Such mechanisms can be specific to a particular application [2], in which case they do not generalize easily, or they can be agnostic to the application as long as the data collection process satisfies the assumptions of the mechanism. In this last case, rewards are typically based on game theoretical approaches [3,4] whose aim is to increase participation of users making rational choices for their own benefit.

E-mail address: tassos.dimitriou@ieee.org.

https://doi.org/10.1016/j.pmcj.2018.07.002
1574-1192/

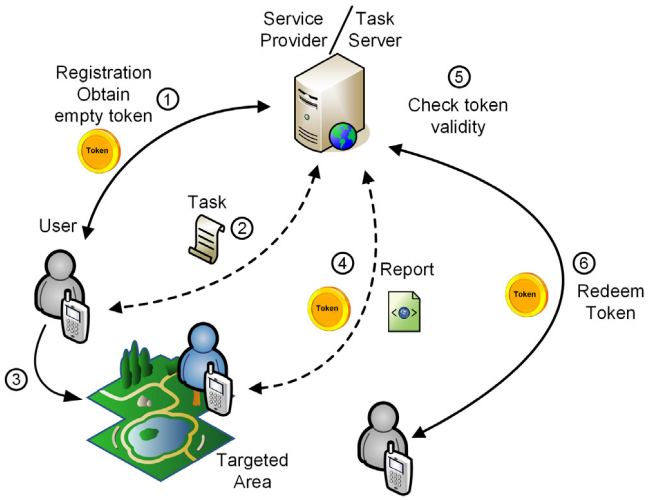

Fig. 1. Acquisition of sensing data, bidding and reporting. Normal arrows indicate items transmitted with real ID. Dashed arrows indicate unlinkable transactions. Token values are always unlinkable.

In this work, however, we will not focus on the incentive mechanisms that can be used to solicit user participation; as mentioned above this is a problem closer to the theory of microeconomics, where demand and supply decide the value of the provided data. Instead, we will focus on the equally important problem of coming up with appropriate mechanisms to *reward* users for the sensed data they submit. Rewarding is a challenging problem as only authenticated users should benefit from the use of such services. On the other hand, the identity of the user or other contextual information should not serve as an identifier that can be used to filter the user's transactions or link it to the rewards collected [5,6].

Contributions: We propose a privacy-preserving scheme of anonymous tokens which can be used by the service provider as a means to reward those users for the data they contributed. During data submission, users earn credits by means of anonymous tokens. Contrary to prior works, however, rewards for different data submissions can be *accumulated* together or even *partially* redeemed. This increases the level of privacy offered by the system as different rewards can be aggregated to a single token, thus reducing the probability of tracking users by the tokens they carry or spend.

Our proposal can be thought as complementary to all approaches that try to enhance user privacy in participatory sensing applications (for a survey see [6]). As most applications collect spatio-temporal information to annotate sensor data, user privacy is put at risk. Hence protection mechanisms are required to ensure that participants' identities cannot be revealed when downloading sensing tasks or reporting sensed data back to the campaign administrators. Our solution integrates nicely with all such proposals whose goal is to ensure anonymity during data submission (see also Fig. 1); every time user data is submitted, our protocol can make sure that an appropriate reward will be credited to an unlinkable token which can be used to aggregate further rewards given to the same (anonymous) user.

We analyze the security of our proposal and we show that such tokens are indeed privacy preserving. In particular, token accumulation does not leak any information about the identity of users and cannot be used in any way by the provider to profile them. Thus our protocols ensure the privacy and unlinkability of transactions. Our work shows that more advanced rewarding mechanisms can be integrated in participatory sensing frameworks, while at the same time offering strong privacy guarantees during the rewarding phase.

Finally, we analyze the efficiency aspects of our proposal; our findings show that our protocols do not incur any significant overhead, and thus can be easily handled by modern-day user devices such as smartphones.

Organization: The remainder of the paper is structured as follows. In Section 2, we review related work on rewarding schemes in urban sensing applications. In Section 3, we introduce our privacy model, we discuss system requirements and assumptions, and we review the basic tools we will be using throughout this work. The details of our privacy-respecting rewarding scheme can be found in Section 4. Its security and efficiency aspects are analyzed in Section 5. Section 6 discusses possible extensions, while Section 7 concludes the paper.

2. Related work

There are many works in the literature whose goal is to motivate users to participate in sensing campaigns. Understanding the reasons why some people may respond to monetary rewards while others may be willing to participate for free, provided they have access to sensed data, is an interesting research question in the area (for a recent survey see [7]). The focus of our work is on the actual rewarding mechanism that can be used to reward users for the data they provide. Prior works do not