Journal of Network and Computer Applications 100 (2017) 24–34

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Privacy-respecting auctions and rewarding mechanisms in mobile crowd-sensing applications

Tassos Dimitriou[a,*,1], Ioannis Krontiris[b]

[a] Computer Engineering Department, Kuwait University, Kuwait
[b] Huawei Technologies Düsseldorf GmbH, Germany

ARTICLE INFO

Keywords:
Mobile crowd sensing
Multi-attribute auctions
Incentive mechanisms
Rewarding
Security and privacy

ABSTRACT

Mobile Crowdsensing (MCS) has emerged as a new paradigm for data collection and knowledge representation, where people use their devices to interact with the environment and create a more accurate picture of their surroundings. In many MCS scenarios it is desirable to give micro-payments to contributors as an incentive for their participation. However, to further encourage participants to use the system, one important requirement is protection of user privacy. In this work we present a *multi-attribute reverse auction* mechanism as an efficient way to offer incentives to users by allowing them to determine their own price for the data they provide, but also as a way to motivate them to submit better quality data. Our auction protocol guarantees bidders' anonymity and suggests a new *rewarding* mechanism that enables winners to claim their reward without being linked to the data they contributed. We have analyzed our protocol and showed that it offers strong security and privacy guarantees in all phases of the auction process, from bidding to rewarding. Additionally, we have implemented the protocol using off-the-shelf cryptographic primitives; our experiments show that the protocol is scalable, it can be applied to a large class of auctions and remains efficient from both a computation and communication point of view so that it can be run to the users' mobile devices.

1. Introduction

The proliferation of devices with sensing capabilities, carried by millions of people, has led to a new sensing paradigm for data collection and knowledge representation where people use their devices to interact with the environment and offer a better understanding of people's activities and their surroundings. This trend is often referred to as Participatory Sensing and Mobile Crowdsensing (MCS) (Guo et al., 2014) or, using the more general term, as Mobile Crowdsourcing (Chatzimilioudis et al., 2012) with typical applications ranging from environmental monitoring, to intelligent transportation and assistive healthcare.

In this paradigm there is a data sharing infrastructure where people can use their devices to collect sensed data and make them available to third parties, and a platform provider who administers this infrastructure and advertises the tasks which people can choose and execute those that match their location and sensing capabilities. However, there are two factors that hinder the large-scale deployment of such applications. First, the lack of proper incentives which does not motivate user participation, and second, the fact that data coming from users' smartphones may have a large impact on their privacy. These two issues have been studied separately in existing research.

From the viewpoint of service providers, monetary incentives could help attract a large number of participants and thereby increase not only the amount of sensed data, but also its quality. As a result a number of MCS systems started incorporating different incentive features, including various forms of rewards based on monetary (Yang et al., 2012), social or gaming-related mechanisms (Di et al., 2013; Sun and Ma, 2014). Some recent work presents an overview of many available incentive mechanisms in MCS till today (Restuccia, 2016; Luo et al., 2017). Micro-payments have been shown to be effective in encouraging participation (Reddy et al., 2010) while Rula et al. (2014) presented additional experimental evidence that such mechanisms can increase the productivity of participants.

One of the challenges in offering micro-payments to contributors is to determine the right amount they expect to receive as a payment for their effort in reporting sensing data. This amount may depend on personal preferences and the perceived cost of their participation, but also on the context and situation users are currently involved which can be different among individuals. One attractive solution to this problem

* Corresponding author.
E-mail addresses: tassos.dimitriou@ieee.org (T. Dimitriou), ioannis.krontiris@huawei.com (I. Krontiris).
[1] Research supported by Kuwait University, Research Grant No. QE 02/15.

http://dx.doi.org/10.1016/j.jnca.2017.10.012
Received 2 March 2017; Received in revised form 29 August 2017; Accepted 19 October 2017
Available online 24 October 2017

is the use of *reverse* auctions, where the auction takes place among data providers (sellers) and data requester (buyers) of sensing data (Yang et al., 2012; Krontiris and Albers, 2012; Lee and Hoh, 2010). This mechanism is more attractive as it eliminates the need for the requester to set or guess the price which users consider reasonable for their data; instead it is the data provider who sets the price for the data it is willing to provide to the requester.

However, as mentioned above, privacy is an important factor that hinders user participation. Collecting data from users' devices has many privacy implications since user-sensitive information such as daily patterns, location and social relationships can easily be deduced from provided data (Christin et al., 2011; Wang et al., 2013; Krontiris et al., 2010). Indeed, as contributed data are strongly related to user activities (e.g., whether the user is at home or at work, walking or driving, whether it's day or night, etc.), daily routines can easily be inferred thus enabling accurate user tracking and profiling. It is thus imperative to address privacy in mobile crowdsensing systems. While several efforts already exist that suggest anonymizing users' contributions to protect user privacy (see for example (Shin et al., 2010)), it still remains an open problem on how to provide privacy protection when incentive mechanisms are also incorporated in the system.

Our Contribution In this work,[2] we suggest a privacy-respecting protocol that allows anonymous users to participate in reverse auctions employed by an MCS system. Our protocol consists of two main parts. The first part provides bidders' anonymity for the auction while it offers guarantees in terms of correctness and fairness of the auction process. The second part explores different options of rewarding users and suggests a new mechanism that enables winners of the auction to claim their rewards without being linked to their contributed data. Thus participants can have the highest privacy assurance, while the MCS platform operator can maintain the flexibility of offering incentives to users and encouraging participation. More specifically, our protocol (i) offers strong privacy protection by guaranteeing user anonymity and unlinkability of transactions, (ii) it is scalable and applicable to typical MCS applications, (iii) it offers resilience to compromised or colluding MCS entities, and (iv) it can support any type of reverse auction. Finally, we have implemented our protocol in a realistic deployment setting, showing the feasibility of our approach.

Organization The rest of the paper is organised as follows. In Section 2, we overview work related to privacy and incentives for MCS systems, while in Section 3, we describe the system and adversarial models for our protocol. In this section we also present a *generic* auction mechanism that does not take privacy into account. Then, in Section 4, we add privacy by describing a scheme that provides for bidder anonymity in MCS auctions as well as different mechanisms that can be used to reward participating users. The protocols' security guarantees and performance are analyzed in Section 5, while Section 6 concludes the paper.

2. Related work

One of the earliest works that addresses the use of incentives for participatory sensing using auctions is Lee and Hoh (2010), in which mobile users sell sensing data to the organizer by bidding their desired selling prices. This work aimed at minimizing platform cost while maintaining a good level of participation, which is obtained by keeping price competition and user retention. Jaimes et al. (2012) observed that for sensing tasks, it is insufficient to select only users with the lowest costs in every round, thus they extended the work of Lee and Hoh (2010) by considering the locations of users, the coverage, and the budget constraint. Thus, this work is the first that brings multi-attribute reverse auctions into the picture. Yang et al. (2012) focused on the truthfulness of the bidding process by designing a reverse-auction mechanism in which bidders cannot improve their utility by submitting bids deviating from their true valued in spite of others' bidding prices. This approach has been further refined in Subramanian et al. (2015).

The above works focused on incentivising users to participate in the sensing tasks without, however, taking into account user differences. For example, some users may be willing to spend more time or efforts in sensing than others do. Multi-Attributive Auctions (MAAs) have thus become a research hot spot, incorporating qualitative attributes to decide the winner (Pham et al., 2015). This was shown to have many advantages for the MCS case, too Krontiris and Albers (2012). In particular, Krontiris and Albers (2012) proposed Multi-Attribute Auctions as a way to consider both incentives of users and multiple attributes of sensed data (for a recent example in the area of visual crowd-sensing see Guo et al., 2016). MAAs constitute an extension of the traditional reverse auction process since a buyer's preferences for an item (its attributes) are also taken into account besides the price (we will talk more about MAAs in Section 3.5). In a simpler setting, Koutsopoulos (2013) considered the case where the main attribute is the quality of sensed data. Thus the system maintains a quality indicator which quantifies the relevance the sensed data provided by the user. Finally, in a recent work (Guo et al.,), Guo et al. have shown how the combination of a reputation and a multi-payment-enhanced reverse auction scheme can be used to improve data quality.

All the above-mentioned works, however, only focus towards providing incentives for stimulating users to participate in mobile crowd sensing applications (see also Zhang et al., 2016 for a more general survey), without however taking the privacy of bids into account.

Privacy is an important requirement in auctions which are used to facilitate the trade of goods. For example, Shi (2013) proposes a sealed bid multi-attribute contract auction protocol that pays special attention on bid privacy and bidder anonymity. However, this and prior work (Peng et al., 2005; Brandt, 2006; Zheng et al., 2007; Nojoumian and Stinson, 2014) on conducting secure auctions has emphasized on attaining full confidentiality in which case bids remain secure even after the auction is over. This is typically achieved by distributing trust among bidders themselves or by using multiple auction servers. As a result, these works rely on heavy cryptographic operations and primitives (e.g. secret sharing techniques, multi-party computations, homomorphic encryption, etc.) and as such they are not considered suitable for Mobile Crowd Sensing applications that require lighter primitives and minimal interaction with other users.

To this end, we have chosen to protect the confidentiality of bids only during the bidding phase. Once this phase is over, all bids are revealed as they don't affect the correctness and fairness of the process or the privacy of users. This model makes sense in the case of multi-attribute auctions as well, since a bid is the value of the utility function which encompasses not only price but other data attributes as well. Despite this, we make sure that privacy and anonymity of participating entities is ensured throughout the auction and rewarding phases of our protocol.

Some generic privacy-respective architectures for MCS exist that could be of interest in our discussion. For example, Gisdakis et al. (2014) recently proposed the SPPEAR architecture, which allows anonymous users to contribute to sensing tasks and receive credits, as long as they submit at least a predefined number of reports. In that sense it supports incentive mechanisms, but it concentrates mainly on the rewarding process without incorporating any auction mechanism. This work has been further extended in Gisdakis et al. (2016), focusing on accountability while at the same time allowing a richer set of incentives to participants.

Another recent work that places emphasis on rewards is given by Li and Cao (2014), who propose two privacy-aware schemes for mobile sensing, where each data provider gets some credit for each contribu-

[2] A preliminary version of this work (Tassos Dimitriou and Ioannis Krontiris, 2015) has appeared in the 9th International Conference on Information Security Theory and Practice (WISTP 2015).