IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON BIG DATA ANALYTICS IN INTERNET OF THINGS AND CYBER-PHYSICAL SYSTEMS

Received December 15, 2016, accepted January 20, 2017, date of publication January 27, 2017, date of current version March 13, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2660461

Quantifying User Reputation Scores, Data Trustworthiness, and User Incentives in Mobile Crowd-Sensing

MARYAM POURYAZDAN[1], (Student Member, IEEE), BURAK KANTARCI[2,3], (Senior Member, IEEE), TOLGA SOYATA[4], (Senior Member, IEEE), LUCA FOSCHINI[5], (Member, IEEE), AND HOUBING SONG[6], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY 13699, USA
[2]School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada
[3]Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY 13699, USA
[4]Department of Computer Engineering, University at Albany, Albany, NY 12222, USA
[5]Department of Computer Science, University of Bologna, Bologna 40126, Italy
[6]Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV 25136, USA

Corresponding author: B. Kantarci (burak.kantarci@uOttawa.ca)

This work was supported by the U.S. National Science Foundation under Grant CNS-1464273 and Grant CNS-1239423.

ABSTRACT Ubiquity of mobile devices with rich sensory capabilities has given rise to the mobile crowd-sensing (MCS) concept, in which a central authority (the platform) and its participants (mobile users) work collaboratively to acquire sensory data over a wide geographic area. Recent research in MCS highlights the following facts: 1) a utility metric can be defined for both the platform and the users, quantifying the value received by either side; 2) incentivizing the users to participate is a non-trivial challenge; 3) correctness and truthfulness of the acquired data must be verified, because the users might provide incorrect or inaccurate data, whether due to malicious intent or malfunctioning devices; and 4) an intricate relationship exists among platform utility, user utility, user reputation, and data trustworthiness, suggesting a co-quantification of these inter-related metrics. In this paper, we study two existing approaches that quantify crowd-sensed data trustworthiness, based on statistical and vote-based user reputation scores. We introduce a new metric—collaborative reputation scores—to expand this definition. Our simulation results show that collaborative reputation scores can provide an effective alternative to the previously proposed metrics and are able to extend crowd sensing to applications that are driven by a centralized as well as decentralized control.

INDEX TERMS Mobile crowd-sensing (MCS), smart city, reputation systems, collaborative sensing, user incentives, reputation score, data trustworthiness, auction theory, social network theory, statistical methods.

I. INTRODUCTION

Mobile Crowd-Sensing (MCS) is an exciting new concept born out of the quest to invent —yet another—transformative Mobile-Cloud application platform, which takes advantage of the exponential global growth in the quantity and popularity of mobile devices [1]. The progress made in the sensory capabilities of today's mobile devices —including cameras, microphones, GPS capabilities, ambient light sensors, accelerometers, digital compasses, and gyroscopes—is staggering [2], enabling a vast variety of MCS applications; one such application, *urban sensing* [3]–[5], prescribes a platform in which volunteering mobile users collect ambient environmental information by downloading an application into their mobile devices and ''opting in.'' The ultimate societal impact of these new crowd-sensing applications—in the areas of public safety, disaster management, and health care—are profound; for example, CreekWatch [6] is an iPhone application developed by the IBM Almaden research center to monitor the conditions of local watershed with the help of crowdsourced data about the amount of water, rate of flow, amount of trash, and a picture of the waterway. Every individual user plays an important role in improving the quality of water resources by sharing captured data with water control boards via the CreekWatch application.

The building blocks of an MCS are the central authority that provides the application (the *platform*) and the participants (the *users*) that contribute their collected data. While some of the users might simply be contributing their data out

2169-3536 © 2017 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

of the goodness of their heart [3]–[7], some are driven by monetary compensation as in the case of Sensing as a Service (S^2aaS) applications [8]. Alternatively, the platform can be a government, non-profit, or a corporate entity providing a free service —by sharing the raw or analyzed data acquired from diverse phenomena [9]—or a commercial entity that is driven by profits [8]. In either case, a *utility* metric can be defined for both the platform and the users, which is not necessarily based on monetary compensation [10]; for example, in [11], an urban resolution metric is introduced to rate the quality of urban sensing services, and in [12], diversity-based quality metric is used to assess the quality of visual crowd-sensed data, i.e., to quantify *platform utility*. Alternatively, the *user utility* has been studied within the context of both monetary compensation [8] and non-monetary awards such as badges [10].

When compensating the participants, the platform makes payments to reputable users contributing useful data; because these payments are made for useful data, we define them as *true payments*. Unfortunately, an unavoidable artifact of an MCS system is the existence of rewards to malicious users who provide bad data; we define these payments as *false payments*. The goal of a successful MCS system is to maximize the true payments and platform utility while keeping user utility at a satisfactory level to encourage healthy participation. Due to the intricate relationship among false payments, true payments, user utility and platform utility, no individual metric can be arbitrarily changed; the goal of this paper is to identify the trade-offs that relate them to one another quantitatively.

Despite its unprecedented ability to help the society, MCS introduces multiple challenges due to its reliance on many ''soft'' factors, such as the willingness of the users to do good for their community. Among such difficulties is the *incentivization* of the users to participate, which is hindered by the heavy computational and communications demand imposed upon by many MCS applications—translating to significantly higher battery power consumption than most of the other smartphone applications; so, unless there are extrinsic motivations for being a member of the MCS platform, most MCS applications are a major turn-off for users due to their battery-unfriendly nature. Since the quality of the collected data depends totally on user participation [11], incentivizing users to participate is a crucial ingredient of a successful MCS system [10], [13]. To increase user participation, various incentive mechanisms have been proposed; auction-based method (reverse auction) [14], [15], game theoretic approaches [10], [16], monetary [15], and non-monetary [17] incentives are among these.

MCS introduces another important challenge: the need to understand user intentions and to quantify their *reputation*. A user might simply think that an MCS application is not good for the community and protest it by contributing incorrect data intentionally or might have a faulty mobile device that takes imprecise or wrong measurements. *Trustworthiness* of the collected data is a primary concern for both the platform and the end users who request sensed data as a service [18]. Kantarci *et al.* [19] study data trustworthiness assurance in user incentivization using statistical- and recommendation-based user reputation-awareness methods, while Social Network-Assisted Trustworthiness Assurance (SONATA) [20] is a recommendation-based approach to identify malicious users who manipulate sensor readings to spread dis-information. SONATA adopts a vote-based trustworthiness analysis and Sybil detection techniques to minimize the manipulation probability in an MCS framework. The study in [21] introduces anchor nodes, which are deployed as trusted entities in an MCS system in order to improve the platform and user utility by eliminating adversaries at the end of a recommendation-based user recruitment process.

Despite the availability of these studies, there is no thorough research stating the specifications for maximum data trustworthiness, high platform utility, and high user utility. In this paper, we formulate *data trustworthiness* as a function of soft reputation and hard reputation of the participants. We quantify *hard reputation* as the accuracy of the sensor readings (e.g., 97%); although this metric is associated with a mobile ''user,'' it is actually based on the sensory accuracy—and functionality—of the mobile ''hardware'' that the associated user employs for participating in the MCS application. Alternatively, we define *soft reputation* to quantify the malicious behavior of the participants —either by their own bad intent or their participation in a malicious group activity [20]. Malicious behavior denotes the manipulation of sensor readings at the mobile application level. We study the viability of statistical, recommendation-based, and anchor-based approaches under collaborative reputation scores in a crowd-sensing system as shown in Fig. 1, which is composed of the platform (the *crowd-sourcer*) and the users (the *sensing data providers*).

Using these three metrics as a guide for quantification, we evaluate the performance of three crowd-sensing approaches via simulations: i) vote-based, ii) anchor-assisted and vote-based, and iii) collaborative reputation scores-based (i.e. hybrid statistical and vote-based). Our simulation results show that applying collaborative reputation scores in user recruitment eliminates the need for trusted entities (i.e. anchors) in the decentralized component of an MCS system without compromising user utility. We also show that the user incentives that employ collaborative reputation scores in user recruitment introduce an additional 5% improvement in the MCS platform utility, while reducing the payments to the malicious users by 10% in comparison to the incentives with decentralized vote-based and anchor-assisted scheme [21].

The rest of the paper is organized as follows. In Section II, we provide background information and related work on MCS research; we particularly focus on the MCS components that directly or indirectly affect crowd-sensed data trustworthiness and user reputation. In Section III, we present different data trustworthiness assurance methods such as statistical reputation-based, vote-based, and anchor-based methods in MCS and highlight their characteristics. Section IV presents

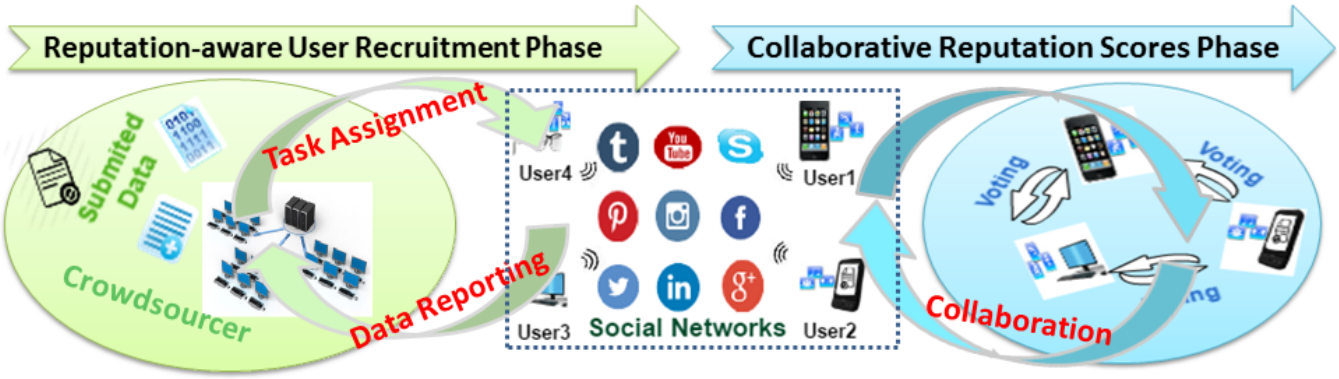


FIGURE 1. Proposed system model. The crowdsourcer (platform) adapts reputation-aware recruitment methods and assigns its participants (users) their sensing tasks. Users collaborate in the trust score phase to ensure data trustworthiness to increase the reliability of submitted data. The quantitative metric, "reputation" of a user, can be calculated solely by the platform (statistical), or by the entire community (vote-based).

collaborative methods to assess user reputation in trustworthy mobile crowd-sensing. In Section V, we present numerical simulation results along with detailed discussions, and finally conclude our paper in Section VI by elaborating on our results and providing directions for future research.

II. BACKGROUND AND RELATED WORK

Gartner estimates that some 3.3 billion of connected mobile devices —with various built-in sensors including GPS, camera, accelerometer, gyroscope, and microphone—will be in operation globally in 2018 [22]. These uniquely identifiable devices [23] are expected to usher in the new era of Internet-of-Things (IoT) and give birth to a new breed of "mobile" applications, be it medical cyber physical systems [24]–[29], smart city [21], or real-time mobile-cloud applications [30]–[32]. One such application is *crowd-sensing*, in which a central authority—acting as the *platform*—employs a group of mobile users —acting as *participants* or *users*— to collect, process, store, and share a large amount of sensory data, thereby forming a Mobile Crowd-Sensing (MCS) system. We must note that the concept of *Crowdsourcing* existed for decades, as evidenced by programs such as SETI @Home [33], in which volunteering participants use their computer time to process extra-terrestrial data in an attempt to find life outside earth. However, *crowd-sensing* expands this concept to beyond what was unimaginable in the SETI @Home days; using mobile devices —rather than computers that sit at home—changes the coverage area of the underlying application from a few fixed points to a smooth and wide geographic coverage, rivaling a coverage percentage that can only be achieved via commercial deployments. This means that commercial-grade sensory data can be collected using everyday mobile users.

A. MCS APPLICATIONS

More than 1.4 B smart phones and 232 M wearable appliances were sold in 2015, while the sales of wearable devices is projected to reach 322 M in 2017 [34]. Various phenomena such as air pollution, water quality, road conditions for smart transportation, public safety, and emergency preparedness can be collaboratively sensed through these devices [9], [35], or environmental monitoring can be performed through autonomous field systems [36]–[38]. MCS has attracted the IT industry for various applications. A research consortium among IBM, University of Illinois, and University of Minnesota has developed a middleware MCS platform, which is called Citizen Sense [39]. Google has developed an MCS application called Science Journal, which is available via Play Store [40]. Science Journal utilizes various built-in sensors in smart-phones to acquire data regarding users' interests and apply real-time analytics.

Zhang *et al.* [41] formulate the life cycle of MCS applications as a four-stage series events with the following stages: i) task creation, ii) task assignment, iii) individual task execution, and iv) crowd-data integration. In each stage, the following 4W1H framework is taken into account: What phenomena should be sensed, when and where the assigned task should be sensed, who is responsible for collecting data, how the sensing task is divided between users, and how collected data is communicated to the recruiter.

Benazzouz *et al.* [42] introduce the term *IoT-centric social networks*, defining a set of connected smart mobile devices that form a social network community by sharing resources and information. In [8], it is stated that the integration of social networks into mobile phone sensing is beneficial for both users requesting MCS services and mobile social network users. In the near future, social networks are expected to connect services and applications over the cloud [43]. As an example of the integration of mobile computing and social networks, MobiGroup [44] is a smart phone sensing system to recommend ongoing activities based on user-activity distance and interaction dynamics in a community. In [45], MCS is used to analyze audio events in social settings.

MCS can also be used to minimize wait time for public services using real-time MCS sensory data. Bulut *et al.* [46] present a crowdsourced wait-time estimation system called LineKing for monitoring and estimating the waiting time to enter a coffee shop. LineKing uses continuous streams of

accelerometer data provided by MCS participants to detect waiting times of users. Another application that applies crowd-powered sensing system to gather and share public information is FlierMeet [47], in which public fliers are collected and shared using the built-in sensors of smart mobile phones. The study in [48] presents a landmark modeling and reconstruction system, which combines user mobility traces, location of captured images, accelerometer, and gyroscope data by the mobile users to build accurate indoor floor plans that improve indoor localization performance. Zhang *et al.* [49] present a self-contained indoor navigation system (GROPING) by using MCS to generate floor maps via three different functions (map building, localization, and navigation). GROPING gathers individual smartphone data via magnetic fingerprints and semantic labels instead of using digitized maps provided by individual venues.

TreSight [50] is an example smart city big data application that uses data analytics and Internet of Things (IoT) to form a recommendation system that aims to improve the smart tourism in the city of Trento, Italy. The output of data analytics can assist decision making processes.

B. COMPONENTS OF MOBILE CROWD-SENSING (MCS)

1) USER RECRUITMENT

Performance of an MCS platform depends on the number of participants contributing to complete sensing tasks. User recruitment—by providing incentives [8], [51]—is a key challenge in an MCS system, permitting the selection of users that are able to fulfill sensing tasks with high accuracy to minimize system costs. Based on how the users are involved in sensing tasks, two main approaches exist: i) in *participatory sensing*, users make the decisions to sense and share data , while ii) in *opportunistic sensing*, mobile devices are involved in the decision making process instead of the users.

2) PLATFORM UTILITY AND USER UTILITY

In an MCS system, the platform generates and assigns tasks, thus incurring a monetary cost to recruit and reward the users for their contribution. On the other hand, users incur costs for their contributions in terms of energy consumed for sensing and data subscription plan use for reporting. Therefore, a "utility" metric can be defined both from the perspective of the platform (*platform utility*) and the users (*user utility*) to quantify the cost vs. reward balance for both sides. Several incentive strategies have been proposed in the literature to address the trade-off between platform and user utility [13]. A mobile agent based approach was proposed in [52] to detect cross-layer anomalies in the received data traffic by using fuzzy logic and rule-based techniques. In [53], new metrics for analyzing MCS datasets were proposed to provide a socio-technical management aspect.

3) TRUE PAYMENTS AND FALSE PAYMENTS

The primary task of the platform is to compensate the users for the data provided by them and compensate them for their participation. Unfortunately because the participants are composed of a mixture of regular and malicious users, making payments to malicious users is an unavoidable consequence of an MCS system, which reduces the platform utility. By using reputation scores, the platform strives to minimize these payments (termed *false payments*) while, at the same time, maximize the payments to regular users (termed *true payments*).

C. FACTORS COMPROMISING USER PARTICIPATION IN MCS

Despite the rapid growth in the popularity of mobile devices, user participation in MCS is still lackluster due to the extensive consumption of time, energy, and bandwidth resources that a typical MCS application requires. Unlike the passive RF devices with μW power power consumption levels [54], crowd-sensing implies power usage in the single-digit Watt range (e.g., 1–10 W), whether implemented with a smartphone or a tablet [38], [55], [56]. Observing that reducing the power consumption of MCS applications will be the primary reason for their wider adoption [9], many studies focused on reducing the mobile power draw during the i) sensing, ii) computing, and iii) data transmission phases of an MCS application.

Energy savings in these individual phases is considered *individual energy conservation methods*, while the *aggregate energy savings* in an MCS application is possible by decreasing the number of recruited nodes. For instance, *coverage-based technique* is adopted in participatory sensing to find the minimum number of participants in order to optimize area coverage [57]. Similarly, the study in [58] minimizes the energy consumption by managing the sensing schedule of each node by duty-cycling the sensing tasks among the participants. *Hierarchical sensing* is a common duty-cycling-based method that transfers data collection from low-level sensors (e.g. accelerometer, WiFi) to high-level sensors (e.g. GPS, Camera) upon failure of the first category to provide accurate sensing information [59]. Chon *et al.* [59] report that hierarchical sensing is not energy efficient because even low-level sensors waste limited battery or save energy just in path tracking. In [60], a parallel transfer and delay tolerant mechanism is used to assign sensed tasks and send back the captured data while users are placing their phone calls to save energy in the data transmission phase.

D. PARTICIPANT SELECTION IN MCS

From the platform's standpoint, a key consideration is the selection of the participants to maximize *platform utility*. A limited number of studies investigate different approaches to address user involvement in MCS to maximize platform utility. The study in [61] presents a participant selection method to choose well-suited users for assigning tasks as well as to consider a reputation management scheme to evaluate the trustworthiness of the contributed data. An experimental MCS study involving 170 participants over a year—named ParticipAct—is introduced in [18] to increase

the effectiveness of data collection by selecting users that are more likely to accept and finalize sensing tasks, based on their historical mobility patterns. ParticipAct compares four different task assignment policies, i) random, ii) recency, iii) frequency, and iv) DBSCAN, to investigate the direct impact of task scheduling on the percentage of success for an MCS system; gamification approaches are utilized involving reputation, ranking, and badges to increase user engagement.

The study in [9] categorizes MCS applications as *personal* and *community* applications based on the participants. *Personal sensing* refers to the acquisition of data related to an individual's daily activities; an analysis of this data can reveal a person's unhealthy habits or health status [62]. *Community sensing* denotes the acquisition of data about popular phenomena involving smart urban services [63], [64], smart transportation [65], or smart cities [66]–[68]. Khan *et al.* [35] present a comprehensive overview on urban sensing. In [69], sensed data is used to design a navigation system (GreenGPS) that recommends the most fuel-efficient route by addressing the sparsity of collected data using a generalized model of complex nonlinear phenomena.

III. REPUTATION AND TRUSTWORTHINESS IN MCS

Verification of the trustworthiness of the data collected by an MCS system is a crucial component of its design, because the collected data can be used to make decisions that affect the quality of life of its participants [27], [71]. Huang *et al.* [72] present a reputation-based system that employs the Gompertz function to determine a "reputation score" for the volunteers that monitor urban noise pollution. Reputation scores are computed in a participatory manner by the participants according to the trustworthiness of the sensed data. The study in [73] proposes a robust trajectory based estimation method within an MCS to handle outliers in the crowdsourced data. The fact that reputation scores cannot be addressed independently from user incentives compounds the difficulties associated with their computation. In this section, we study reputation scores in two categories: i) *statistical reputation scores* that are solely computed by the platform and ii) *vote-based reputation scores* that are computed by the participants of the MCS. Table 1 tabulates the notation used throughout the rest of the paper, along with the equation and section numbers in which these notations are used.

A. DEFINITIONS FOR REPUTATION VS. TRUSTWORTHINESS

In this subsection, we provide a high level definition of the two key terms of our study, namely *user reputation* and *data trustworthiness*. We associate the *reputation* attribute with a mobile user, while the *trustworthiness* is an attribute that is associated with the data a given user collects; hence, based on these definitions, the *data trustworthiness* is a direct consequence of *user reputation*. We further expand on this definition to include two primary factors that contribute to user reputation: i) to capture the sensory accuracy or the possibility of an outright device malfunction, we define the metric *hard reputation* (R^{hard}), which quantifies the accuracy and functionality that is expected from a mobile device associated with a specific participating MCS user (or more generally a *sensing node*) and ii) to capture the average probability of inaccurate—or outright wrong—readings that stem from malicious intelligence (either malicious users manipulating readings or a virus causing incorrect reporting), we define the metric *soft reputation* (R^{soft}). What follows from these two definitions is that the *data trustworthiness* of user i ($\mathfrak{T}_i$) is a function of the hard (R_i^{hard}) and soft (R_i^{soft}) reputation of that user as formulated in Eq. 1:

$$\mathfrak{T}_i = f(R_i^{hard}, R_i^{soft}) \tag{1}$$

By definition, R_i^{hard} captures inaccuracies that stem from hardware based errors that are *predictable*. Therefore, they can be quickly detected by using statistical methods. On the other hand, inaccuracies that arise from R_i^{soft} involve some sort of a malicious *intelligence*, thereby making them *unpredictable*. To phrase alternatively, R_i^{soft} involves the *trustworthiness* of the data, while R_i^{hard} represents its *correctness*. Although it is possible to study the effects of these two factors on trustworthiness separately, we focus our attention on R_i^{soft} and view R_i^{hard} as a limiting condition; as long as the accuracy of the hardware sensors of user i's device (ϱ_i) is above a certain threshold (ϱ^{TH}), the trustworthiness of the data acquired by user i ($\mathfrak{T}_i$) can be assumed to be dictated solely by the soft reputation of user i as formulated in Eq. 2:

$$\mathfrak{T}_i = \begin{cases} f(R_i^{hard}, R_i^{soft}), & \varrho_i < \varrho^{TH} \\ R_i^{soft} = R_i, & \varrho_i \geq \varrho^{TH} \end{cases} \tag{2}$$

In this paper, given that the accuracy of modern smartphone sensor readings is at the level of 97–98% [70], we assume that the condition, $\varrho_i \geq \varrho^{TH}$ is met in real systems, which enables us to assume that the trustworthiness of a user's data is directly proportional to the reputation of that user. In other words, we assume that the quantities $\mathfrak{T}_i$, R_i, and R_i^{soft} are *statistically equivalent*.

B. STATISTICAL (CENTRALIZED) REPUTATION-BASED MCS

In [74], Trustworthy Sensing for Crowd Management (TSCM) is proposed for the recruitment of smartphone users based on a reverse auction procedure executed in the cloud. TSCM introduces reputation-awareness and trustworthiness into MSensing auction-based incentives [75] by considering both past and recent sensor readings. According to TSCM, inaccurate or manipulated information readings lead to reputation reduction for a given user i, consequently reducing the trustworthiness of the data provided by user i. An "auction" is a two-step procedure to select reputable users among all participating users, which seeks to meet the utility requirements of the selected users and the platform.

Each sensing task has a value for the crowdsourcer platform. Recruitment of a set of smartphone users in a crowdsensing campaign corresponds to a value which is the total

TABLE 1. Notation used throughout the paper including references to which equation – and section – they appear in.

NOTATION	EQUATIONS	SECTIONS	DESCRIPTION
$\mathfrak{T}_i$	2	3.1	Trustworthiness of data acquired through user i
R_i^{hard}	2	3.1	Hardware reputation of the mobile device of user i
R_i^{soft}	2	3.1	Soft (i.e., intelligence-related) reputation of user i
ϱ_i	2	3.1	Sensor accuracy for user i's mobile device (typically 97–98% [73])
ϱ^{TH}	2	3.1	Sensor accuracy threshold for R^{soft} to represent the entire reputation
T_X	3; 5; 10; 13; 15; 16; 17	3.2; 3.3; 3.4; 4	Set of tasks handled by the users in the set X
W	3; 4; 5; 9	3.2	Generic symbol for set of winners
W^τ	17; 18; 19	4; 5	Set of winners at τ^{th} recruitment
$\widehat{W}_i$	10; 13	3.3; 3.4	Community that votes for the reputation of user i
w_i	10; 11; 13; 14; 15; 16	3.3; 3.4; 4	Vote capacity of user i
w_i^-	10; 14	3.3; 3.4	Previous vote capacity of user i
w_i^{inst}	13; 14	3.4	Instantaneous vote capacity of user i
χ_j^i	11; 15; 16	3.3; 4	Actual vote of user j for user i
b_i	8; 9; 20	3.2; 5.3	Generic symbol for the sensing cost (bid) of user i
b_i^τ	19	5;	Sensing cost (bid) of user i at τ^{th} recruitment
t	6; 7	3.2	Sensing campaign time
τ_{total}	19	5	Duration of τ^{th} recruitment
$p_i(t)$	6; 15; 16	3.2; 4	Positive readings of user i at time t
$n_i(t)$	6; 15; 16	3.2; 4	Negative readings of user i at time t
$\mathrm{P}_i{}^\tau$	18; 19	5	Total Payment to user i at τ^{th} recruitment
v_T	3; 5	3.2	Value of task T in the platform
$v^R(W)$	4 ; 5	3.2	Reputation based value of the tasks sensed by the set of users W
$v^R(W^\tau)$	17; 18	4; 5	Reputation based value of tasks sensed by user set W at τ^{th} recruitment
$v_i^R(W)$	4 ; 5; 9; 20	3.2; 5.3	Reputation based marginal contribution of user i to user set W
v_{wv}^R	8	3.2	Reputation based marginal contribution of user V to recruited set $\{W-w\}$
$R_i(t)$	7; 12	3.2; 3.4	Reputation of user i at the end of time t
R_i	5; 8; 9; 11; 16	3.2; 3.3; 4	Generic symbol for the reputation of user i
$R_i(t^-)$	7; 12	3.2; 3.4	Reputation of user i immediately before t
$R_i^{inst}(t)$	7; 12	3.2; 3.4	Instantaneous reputation of user i calculated at t
R_i^{voted}	11; 16	3.3; 4	Voted (decentralized) reputation of user i
R_i^{stat}	6; 16; 17	3.2; 4	Statistical (centralized) reputation of user i
R_i^{coll}	15; 16; 17; 20	4; 5.3	Collaborative reputation score of user i
$R_i^{coll_{inst}}$	15; 16	4	Instantaneous collaborative trust score of user i
Γ_{T}	5; 17	3.2; 4	Set of users handling task T
ϵ	6; 15; 16	3.2; 4	Bayesian estimation factor
$\delta, 1-\delta$	7; 12; 15; 16	3.2; 3.4; 4	Weights of current (δ) and previous ($1-\delta$) reputations
$\gamma, 1-\gamma$	10; 14	3.3; 3.4	Weights of current and previous vote capacities
$\sigma, 1-\sigma$	16	4	Weights of centralized and decentralized reputation components
$U_{platform}$	18	5	Platform utility
U_{user}	19	5	User utility

value of the tasks that are sensed by the recruited users in a participatory manner. we define a *sensing campaign* as a consecutive set of sensing tasks that are executed sequentially. TSCM uses the reputable marginal value ($v_i^R(W)$) of user i on set W as formulated in Eq. 3. Reputable marginal value denotes the additional value introduced by user i to the reputable value of set W; it is calculated by summing the values of the tasks forming the sensing set as shown in Eq. 4.

Additionally, the value of a task is defined by its actual value scaled by the average reputation of the users as formulated in Eq. 5.

$$v(W) = \sum_{\mathrm{T} \in T_w} v_{\mathrm{T}} \tag{3}$$

$$v_i^R(W) = v^R(W \cup \{i\}) - v^R(W) \tag{4}$$

$$v^R(W) = \sum_{\mathrm{T} \in T_W} \sum_{k \in \Gamma_{\mathrm{T}}} \left(v_T . R_k / |\Gamma_{\mathrm{T}}| \right) \tag{5}$$

Statistical reputation of user i (R_i^{stat}), computed from Eq. 6, correlates positive readings ($p(t)$) to total readings ($p(t)+n(t)$) as follows:

$$R_i^{stat}(t) = \frac{p_i(t) + \epsilon}{n_i(t) + 2\epsilon} \tag{6}$$

where ϵ comes from Bayesian estimation of a binary random variable. Thus, eventually the probability of having a true reading is expected to be equal to Eq. 6. TSCM continuously assesses the instantaneous reputation of a user i at time t ($R_i(t)$) by using a running average sum of their current—or *instantaneous*—($R_i^{inst}(t)$) and past reputation scores ($R_i(t^-)$) as formulated in Eq. 7:

$$R_i(t) = \delta . R_i^{inst}(t) + (1 - \delta) . R_i(t^-) \tag{7}$$

where the δ parameter is introduced to model the transition probability of user reputations (see Table 1). TSCM, much like its predecessor MSensing, ensures that all participants are compensated with amounts that are no less than their sensing costs. While recruiting users, the platform aims to recruit users whose reputable marginal values are greater than their modified bid as formulated in Eq. 8:

$$\left(\frac{v_{wv}^R - b_{wv}}{R_{wv}}\right) > \frac{v_{wv+1}^R - b_{wv+1}}{R_{wv+1}} \tag{8}$$

While the schemes that are explained in this section adopt MSensing to incentivize users, participant recruitment phase is based on a reverse auction procedure [75]. User recruitment phase consists of two steps: 1) winner selection and 2) payment determination. In step (1), the platform selects the winner set of users based on their marginal contribution as formulated in Eq. 9. The aggregate reputation of the set of selected users is the summation of their reputation over the average reputation of the winner set, where b^i represents the bid (sensing cost of the user) divided by the user's reputation R^i.

$$v_i^R(W) - \frac{b_i}{R_i} \tag{9}$$

The frameworks presented in this section adopt the payment determination phases in [74] and [75]. Once the winners are selected, step (2) is the payment determination (i.e., compensation) for the winners. To this end, for each selected mobile device, w, the platform first constructs a temporary set of non-winner mobile devices/users where each mobile device has a positive reputation-based contribution to the value of the set of recruited users. Next, the set of recruited users is gradually re-built by searching for the maximum possible sensing cost for a mobile device that will still make it preferable over any other mobile device in the set of non-winners. The corresponding value is assigned as the payment to the mobile device user.

C. VOTED (DECENTRALIZED) REPUTATION

A mobile social network is formed by its participants to perform common sensing tasks and share the crowd-sensed data. In such a platform, user reputations can be calculated by the participating users in a *decentralized* fashion —rather than the platform itself—by means of a *voting* procedure. Kantarci *et al.* [19] propose Social Network-Assisted Trustworthiness Assurance (SONATA) to incentivize and recruit trustworthy users through a fully decentralized reputation-aware method, which consists of four components: i) the cloud computing *platform*, ii) *mobile social networks* (i.e., communities), and mobile device users that are considered either iii) *sensing providers*, or iv) *service requesters* for different tasks.

SONATA integrates mobile user reputation awareness into MSensing [75], which is a reverse auction-based approach as mentioned earlier; although SONATA allows every user to vote for the reputation of their neighbors, it detects Sybil attacks by using methods that are proposed for online social networks [77]. Malicious users that aim to join the network with the intention to spread dis-information are considered to be analogous to the Sybil users in online social networks. The vote of a mobile user for any neighbor is either 1 or -1, where 1 denotes positive reputation indicator (i.e. non-malicious user) or vice versa. SONATA builds a set of winners based on maximizing the marginal contribution to the platform utility. Marginal contribution is calculated according to difference between two different values of the winning set before and after joining the newcomer users to the winner set (W) as explained earlier.

As mentioned earlier, in the decentralized reputation model, users with common sensing tasks form a social network where each node in the network is eligible to vote for the other nodes to build their reputation by the end of the recruitment period. Alternatively, in the decentralized reputation model, each user i has a vote capacity (w_i) and it is a weighted sum of the current vote capacity (ω_i^-) and the sum of the gained vote capacities from its neighbor nodes normalized by the number of connected users in the social network as formulated in Eq. 10:

$$\omega_i = \gamma . \omega_i^- + (1 - \gamma) . \sum_{k | T_i \cap T_j \neq 0} \left(\omega_k / |\widehat{W}_i| \right) \tag{10}$$

where γ denotes the vote capacity transition constant. We define the instantaneous voted (decentralized) reputation of a user (R_i^{voted}) as the ratio of the weighted sum of the votes cast by the voting neighbors to the weighted sum of the reputations of the voting users. As formulated in Eq. 11, weight of each vote cast by a voting neighbor is equal to the

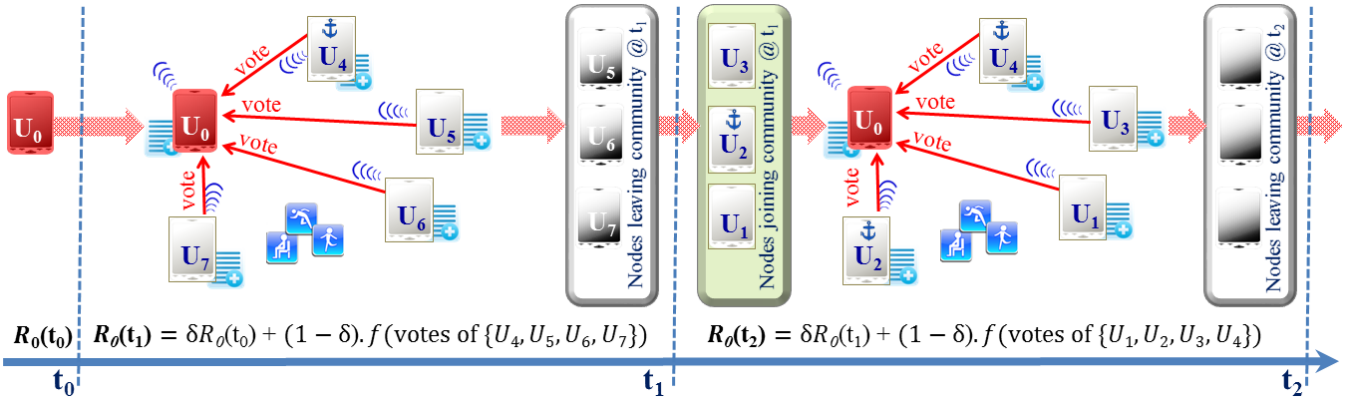


FIGURE 2. An example scenario for anchor-assisted vote-based reputation scores. U_2 and U_4 are the trusted entities (*anchor* nodes [21], [76], denoted by an anchor symbol) in the crowd-sensing terrain. At times t_1 and t_2, all nodes vote for the reputation of U_0, regardless of whether they are an anchor or a regular node. The decentralized reputation score of U_0 is calculated based on a weighted sum of its previous and current reputation scores. Current reputation is calculated on the basis of the vote capacities and votes cast by the nodes in the same community at t_2, i.e., $\{U_1, U_2, U_3, U_4\}$.

product of the vote capacity of the corresponding neighbor and its reputation.

$$R_i^{voted} = \frac{\sum_{k|(C_{ik})=1} \left(\omega_k . X_i^k . R_k\right)}{\sum_{k|T_i \cap T_K \neq 0} \left(\omega_k . R_k\right)} \tag{11}$$

D. ANCHOR-ASSISTED DECENTRALIZED REPUTATION

To improve data trustworthiness assessment in the decentralized vote-based approach, Pouryazdan *et al.* [21] proposed to assign the *anchor* role to a small set of nodes. Anchor nodes have 100% vote capacity, 100% reputation, and are considered to be 100% trustworthy in an MCS platform. They are recruited exactly the same as the non-anchor nodes and their reputation-based contributions and/or bids are identical to their reputation-unaware ones as they are presumed to be 100% trustworthy until the end of a monitoring period.

As the communities vary dynamically, reputation of user i ($R_i(t)$) is characterized by the instantaneous reputation at time t ($R_i^{inst}(t)$) and overall reputation at time t^- ($R_i(t^-)$). $R_i^{inst}(t)$ is computed as the weighted sum of the votes of all nodes in the community scaled by the sum of the vote capacity of the users that cast votes as formulated in Eq. 12, where δ denotes the transition coefficient for reputation to capture the rate of change in $R_i(t)$ between t and t^-; 100% trustworthiness is assumed for all anchor nodes.

$$R_i(t) = \begin{cases} \delta . R_i^{inst}(t) + (1-\delta) . R_i(t^-), & i \in U \text{ users} \\ R_i^{inst}(t) = R_i(t^-) = 1, & i \in A \text{ anchors} \end{cases} \tag{12}$$

Besides their reputation, each user also has a *vote capacity*, which is updated dynamically based on the votes distributed by the neighbors in the same community. By joining a new community, instantaneous vote capacity of a new user is calculated in Eq. 13 as the average vote capacity of its connections, i.e., the nodes that have already cast votes for the newly joining node. We note here that the vote capacity of anchor nodes is always 1 and is independent of the votes.

$$\omega_i^{inst} = \begin{cases} \sum_{k|T_i \bigcap T_k \neq 0} \left(\omega_k / |\widehat{W}_i|\right), & i \in U \text{ users} \\ 1, & i \in A \text{ anchors} \end{cases} \tag{13}$$

On the other hand, the actual vote capacity of a node is the weighted sum of its instantaneous vote capacity and prior total vote capacity, based on the transition coefficient of reputation γ as formulated in Eq. 14. In the equation, the instantaneous vote capacity (ω_i^{inst}) is formulated by the second summation component of Eq. 10.

$$\omega_i = \gamma \cdot \omega_i^- + (1-\gamma) \cdot \omega_i^{inst} \tag{14}$$

Figure 2 is an illustrative MCS example, in which user 2 (U_2) and user 4 (U_4) are considered to be anchor nodes. At $t = t_1$, U_0, with an initial reputation value $R_0(t_0)$, joins the community with four nodes: $\{U_4, U_5, U_6, U_7\}$. At the end of t_1, the reputation of U_0 is a weighted sum of its initial reputation and a function of its newly voted reputation. The vote reputation of U_0 is contributed by the votes of U_4, U_5, U_6, and U_7. At t_1, upon reporting their sensing tasks, U_5, U_6, and U_7 leave the community, i.e., quit participating in the sensing campaign. At $t = t_2$, a new sensing task is scheduled within a sensing range covering $\{U_0, U_1, U_2, U_3, U_4\}$. Given that U_0 does not have any common tasks with the nodes in this new community, $\{U_1, U_2, U_3\}$ vote for the trustworthiness of U_0. Since U_4 is an anchor node, it also votes for the reputation of U_0 Finally, a weighted sum of U_0's reputation at t_1 and its voted reputation at t_2 are stored as its overall reputation score at $t2$.

IV. COLLABORATIVE REPUTATION SCORES

Previous user recruitment schemes rely on either centralized (statistical) or decentralized (vote-based) trustworthiness

assurance in MCS systems. Each approach has its own pros and cons; decentralized trustworthiness assurance delegates the storage and computational load on the central platform to the mobile devices, while centralized trustworthiness assurance keeps track of the historical behavior patterns, which—in the long run—can significantly improve platform utility by eliminating the users that provide wrong sensor readings. The decentralized approach can converge to providing a stable platform utility under medium loads (i.e. task arrival rates), owing to its delegation of the user reputation assessment to the community. Combining decentralized and centralized methods for reputation-aware user recruitment in MCS can consolidate the benefits of both approaches. In this section, we present an approach to obtain collaborative reputation scores, which are a weighted function of the decentralized and centralized reputation components in user recruitment.

The instantaneous reputation of a user i is a compound function of its statistical reputation (R_i^{stat}, as defined in Eq. 6 as the ratio of positive readings to the total readings) and its social reputation ($R_i^{voted}(t)$) as formulated in Eq. 15.

$$R_i^{coll_{inst}} = \left[(1-\delta)\cdot\left(\frac{p_i(t)+\epsilon}{p_i(t)+n_i(t)+2\epsilon}\right) + \delta\cdot\frac{\sum_{k|T_{\{i\}}\cap T_{\{k\}}\neq\phi}\left(\omega_k\cdot\chi_k^i\cdot R_k\right)}{\sum_{k|T_{\{i\}}\cap T_{\{k\}}\neq\phi}\left(\omega_k\cdot R_k\right)}\right] \quad (15)$$

Kantarci *et al.* [19] propose a social network theory-based collaborative trustworthiness approach, which leverages the naive centralized reputation value by incorporating statistical reputation scores and vote-based reputation scores. We refer this method as the *collaborative reputation scores approach*. This approach is similar to SONATA [20], in which users with common sensing tasks are eligible to cast votes for other nodes in the same social community while, at the same time, the MCS platform considers all statistical information about both past and recent sensor readings of users. Note that in the statistical reputation, positive and negative readings are identified after running an outlier detection procedure [78], by marking the outliers as negative readings. The formula for the collaborative reputation of user i ($R_i^{coll}(t)$) is obtained from the weighted sum of the previous and current reputation as formulated in Eq. 16.

Collaborative reputation scores-based user recruitment also adopts TSCM steps for winner selection and user rewarding. However, in such a system, as opposed to the previous systems that are based on either centralized or decentralized reputation assessment, the method to assess the value of the crowd-sensed data is not straightforward as the decentralized component can be biased while the centralized component is mostly unbiased.

$$\begin{aligned} R_i^{coll}(t) &= \sigma R_i(t^-) + (1-\sigma)\cdot R_i^{coll_{inst}} \\ &= \sigma\cdot R_i(t^-) + (1-\sigma)\cdot\left[(1-\delta)\cdot R_i^{stat}(t) + \delta\cdot R_i^{voted}(t)\right] \\ &= \sigma\cdot R_i(t^-) + (1-\sigma)\cdot\left[(1-\delta)\cdot\left(\frac{p_i(t)+\epsilon}{p_i(t)+n_i(t)+2\epsilon}\right) + \delta\cdot\frac{\sum_{k|T_{\{i\}}\cap T_{\{k\}}\neq\phi}\left(\omega_k\cdot\chi_k^i\cdot R_k\right)}{\sum_{k|T_{\{i\}}\cap T_{\{k\}}\neq\phi}\left(\omega_k\cdot R_k\right)}\right] \end{aligned} \quad (16)$$

In this paper, we present two different modes to assess the value of a recruited crowd when collaborative reputation scores are applied. Equation 17 formulates the value of a recruited crowd in two different modes at the τ^{th} recruitment. In the first mode (M_1), the value of the recruited crowd is calculated based on the collaborative user reputation values. Thus, the value of a crowd-sensed task is scaled by the average collaborative reputation of the users who have sensed the task in a participatory manner. In other words, the value function has both unbiased and possibly biased components. In the second mode (M_2), the value of the crowd-sensed data is calculated by scaling the total value by the average statistical reputation of the users who have sensed the task in a participatory manner. Thus, the second mode aims to remove possible community bias from the value calculation.

$$v^R(W^\tau) = \begin{cases} \sum_{T\in T_{W^\tau}}\sum_{k\in\Gamma^\tau}\left(v_T.R_k^{coll}/|\Gamma^\tau|\right), & \text{mode}M_1 \\ \sum_{T\in T_{W^\tau}}\sum_{k\in\Gamma^\tau}\left(v_T.R_k^{stat}/|\Gamma^\tau|\right), & \text{mode}M_2 \end{cases} \quad (17)$$

The aim of this paper is to study the impact of decentralized and centralized components in trustworthiness assurance in mobile crowd-sensing and provide design specifications to meet the platform utility, user utility, and data trustworthiness goals in these applications. To this end, the next section provides a thorough performance study of the presented schemes.

V. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed user recruitment schemes in MCS systems via simulations. We aim to quantify the user reputation and data trustworthiness under statistical and collaborative methods for user recruitment in MCS. Furthermore, we investigate the impact of deploying anchor nodes as the trusted entities to improve the reputation of the recruited user sets. In our simulated scenarios, users are recruited based on collaborative reputation scores with/without anchor nodes (i.e., trusted entities) [19], [21] and TSCM [74].

TSCM, which employs statistical reputation maintenance, is a reputation-aware version of MSensing [79] whereas SONATA uses a fully decentralized approach to obtain user reputation and assess the reputation-based value of the crowd-sensed data. Social Network-Assisted Trustworthiness Assurance (SONATA) has a decentralized nature such that users cast votes for their neighbors in same community [20]. As shown in [19], introduction of collaborative reputation scores improves the performance of TSCM and SONATA in terms of platform utility and data trustworthiness by reducing the payments to malicious users. In this evaluation, we compare the performance of TSCM and collaborative reputation scores. In the performance comparison, we consider two operation modes for collaborative methods —M_1 and M_2—as formulated in Eq. 17. The M_1 mode uses collaborative reputation scores of the users to assess the reputation of a recruited crowd whereas the M_2 mode keeps track of the statistical reputation of each user in the crowd for the same purpose. In all test scenarios, we use TSCM as the benchmark scheme, which is based entirely statistical reputations of users.

A. SIMULATION SETUP

For simulations, we use the same simulation settings in [21] on a Java-based discrete event simulator that we developed. All simulations run at a terrain that covers a 1000 m×1000 m geographic area with 1000 smartphone participants. Each sensing event lasts for 30 minutes and the arrival rate of sensing tasks takes its value from the set {20, 40, 60, 80, 100} tasks/min following a Poisson distribution.

The value of a sensed task varies between 1 to 5 and the sensing cost of a mobile user is distributed uniformly in [1, 10]. We set the ratio of malicious smart-phone users (i.e., probability of malicious nodes) to 3% and 5% of the entire crowd population. Furthermore, in the case of anchor-assisted and vote-based trustworthiness assurance, we set the anchor percentage in the crowd (i.e., anchor nodes) to 3% and 5% of the entire crowd population. Table 2 summarizes the simulation settings that have been applied in the evaluation of the proposed methods in detail. Each scenario has been run with five different seeds, and the result charts present the average of five runs in the simulation results section. Using this setup, we now report our evaluation results for the three metrics introduced in Section V-B.

B. EVALUATION METRICS

We aim to find the design specifications and conditions for user recruitment that would result in high utility for the platform and the users, as well as high trustworthiness of the crowd-sensed data. We base our simulations on three inter-related metrics: i) *platform utility*, ii) *average user utility*, and iii) the *total payment to malicious users*. While the design goal of an MCS is to maximize (i) and (ii), a side-effect of most of the previously described algorithms is the unavoidable introduction of (iii), i.e., payments made to users that provide biased, incorrect, or misleading data.

TABLE 2. Simulation setup.

PARAMETER	VALUE
Terrain Size	1000 m × 1000 m
Sensing Range	30 m
Number of Users	1000
Task Arrival Rates	20; 40; 60; 80; 100/min
Initial reputation of a newcomer	0.3; 0.5; 0.7
Malicious user probability	0.05
Anchor probability	0.05
Task Value	{1; 2; 3; 4; 5}
Accuracy of built-in sensors (ϱ)	$\varrho \in$ [0.97– 0.98]
Bid value	{1; 2; ...; 10}
Adversary Detection Probability	0.20
Sensing inaccuracy probability	[0.02, 0.03]
Reputation Transition Coefficient	0.5
Simulation Duration	30 min

Platform utility ($U_{platform}$) denotes the total received value from the participants deducted by the total payments awarded to the users. Here, it is worthwhile noting that in the case of trustworthiness assurance through collaborative reputation scores, the value of the recruited crowd at time τ ($v^R(W_\tau)$) may denote either the value calculated through collaborative reputation scores (i.e., M_1 mode) or the usefulness of data which is totally based on a centralized outlier detection procedure (i.e., M_2 mode). Platform utility is formulated in Eq. 18. We provide our evaluation results for this metric in Section V-C.

$$U_{platform} = \sum_{\tau} \left(v^R(W^\tau) - \sum_{k} {P_k}^\tau \right), \tag{18}$$

Average user utility (U_{user}) denotes the difference between the payment received from the platform and the sensing cost per user per sensing campaign as formulated in Eq. 19. We provide our evaluation results for this metric in Section V-D.

$$U_{user} = \frac{\sum_{\tau} \left(\left(\sum_{k} {P_k}^\tau - \sum_{k} {b_k}^\tau \right) / |W^\tau| \right)}{\tau_{total}}. \tag{19}$$

In both Eq. 18 and Eq. 19, ${P_k}^\tau$ is the total payment to user k whereas ${b_k}^\tau$ (in Eq. 19) is sensing cost (bid) of user k during τ. The parameter W_τ represents the set of winners during the auction period τ_{total}, which denotes the total number of sensing campaigns.

False Payments (Total amount of payment to malicious users) denotes the rewards given to malicious users. The platform aims at minimizing this parameter in order to improve the trustworthiness of the collected data. We provide our evaluation results for this metric in Section V-E.

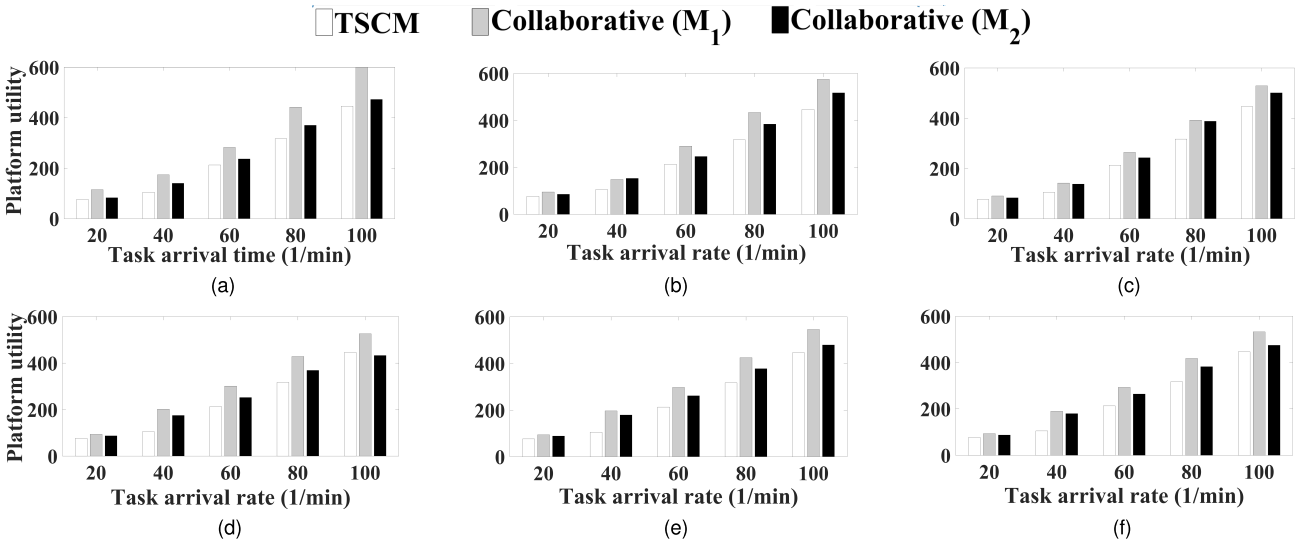


FIGURE 3. Platform Utility vs Sensing Task Arrival Rate. The sub-figures in (a)–(c) depict a deployment without anchors with the following initial reputation scores for the newly joining participants: a) $R_i(0) = 0.3$, b) $R_i(0) = 0.5$, c) $R_i(0) = 0.7$. Because no anchor nodes are deployed as trusted entities in (a)–(c), $\omega_i^{inst} \leq 1$ (per Eq. 14). The sub-figures in (d)–(f) depict a deployment with anchor nodes with the initial reputation scores d) $R_i(0) = 0.3$, e) $R_i(0) = 0.5$, f) $R_i(0) = 0.7$. The impact of the initial reputation—$R_i(0)$—is more significant when the users are recruited on the basis of collaborative reputation scores (per Eq. 16), and while the value of the recruited crowd ($v^R(W^\tau)$) is obtained via collaborative reputation scores (M_1 in Eq. 17). In the M_2 mode, nodes build reputation slower as their sensed tasks are valued only based on statistical reputation (M_2 in Eq. 17). Regardless of the mode (M_1 or M_2), $R_i(0) = 0.7$ with collaborative reputation scores leads to the highest improvement in platform utility. The deployment of anchor nodes in (d)–(f) does not introduce significant improvement to platform utility when compared to the scenarios in (a)–(c).

Before we proceed with the simulation results, we present a brief discussion on the theory of crowd-sensing. As seen in Eq. 18, the platform aims to recruit users that introduce higher marginal contribution and lesser sensing costs. As seen in Eq. 9, marginal contribution of a user is not only a function of the value of the sensed data and its cost but also a function of the user's reputation score, which can be obtained via statistical, collaborative or hybrid methods. The higher the user reputation is, the lesser the modified bid of the user. Consequently, the lesser the modified bid of the user, the higher the marginal contribution of the corresponding user, as well as the higher the platform utility. Thus, a higher user reputation score is expected to lead to a higher platform utility. On the other hand, Eq. 19 states that user utility increases with payments received from the platform and with lower sensing costs (i.e., bids). Thus, there exists a trade-off between platform utility and user utility. This is why we apply a reverse auction between the platform and the users. It is worth noting that low reputation scores also lead to lower payments and consequently lower user utilities.

C. EVALUATION: PLATFORM UTILITY

In Fig. 3, the impact of using collaborative reputation scores under the two value assessment modes—M_1 and M_2—is presented when user i is assigned an initial reputation $R_i(0) = 0.3$ when participating in the first crowd-sensing campaign. In Fig. 3, the term *collaborative* denotes that the reputation assessment under SONATA is consolidated with the statistical reputation; using collaborative reputation scores (R_i^{coll}) in the M_1 mode leads to the highest platform utility under all initial reputation values, $R_i(0) \in \{0.3, 0.5, 0.7\}$. The scenarios in Fig. 3 a–c do not deploy anchor nodes to obtain collaborative reputation scores. Thus, in the decentralized component of reputation calculation, the instantaneous vote capacity of each node may vary (i.e., $\omega_i^{inst} \leq 1$ per Eq. 14). Furthermore, the impact of $R_i(0)$ (initial reputation) of the newly joining users is more significant when the users are recruited on the basis of the collaborative reputation scores (see Eq. 16) while the value of the recruited crowd ($v^R(W^\tau)$) in the sensing campaign τ is obtained via collaborative reputation scores (M_1 in Eq. 17). In the M_1 mode, the value of the recruited crowd is calculated based on the users' collaborative reputation scores (R_i^{coll} in Eq. 16) and in the winner selection state, sensing costs, as well as the reputation-based task values are adjusted based on the collaborative reputation scores. Thus, marginal contribution in Eq. 9 becomes the following:

$$v_i^R(W) - \frac{b_i}{R_i^{coll}} \tag{20}$$

On the other hand, under the M_2 mode, while the malicious nodes can be identified using the combined the statistical and vote-based information, collaborative reputation scores affect the bids (costs) of the participants. Furthermore, the centralized component (i.e. statistical reputation) affects the value of the crowd-sensed tasks as formulated in Eq. 17. Consequently this causes the nodes to build reputation slower than the case when the platform calculates the reputation-based values under the M_2 mode. Nevertheless, when $R_i(0)$ is set to 0.7 for each newly joining participant, employment of collaborative reputation scores improves the platform utility

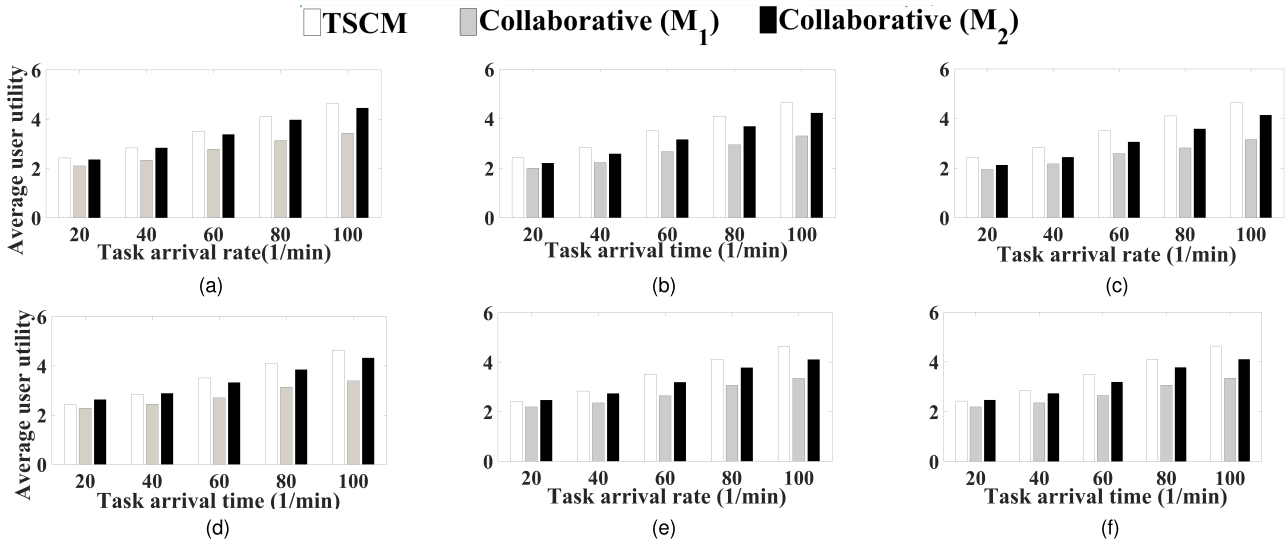


FIGURE 4. User Utility vs. Sensing Task Arrival Rate. The sub-figures in (a)–(c) depict a deployment without anchors with the following initial reputation scores for the newly joining participants: a) $R_i(0) = 0.3$, b) $R_i(0) = 0.5$, c) $R_i(0) = 0.7$. The sub-figures in (d)–(f) depict a deployment with anchor nodes with the initial reputation scores d) $R_i(0) = 0.3$, e) $R_i(0) = 0.5$, f) $R_i(0) = 0.7$. Collaborative reputation scores in Eq. 16 lead to significant cuts to user utility in both non-anchored and anchored scenarios. These cuts can be limited when the value of the recruited crowd—$v^R(W^\tau)$—is calculated based on the statistical reputation (per Eq. 17, M_2 mode). Because mode M_1 in Eq. 17 uses vote-based and statistical reputation components to obtain the value of the recruited crowd, the votes for the neighbors (χ_j^i in Eq. 17) can be biased, which may result in reduced $R_i^{voted}(t)$ (reputation component) of $R_i^{coll}(t)$ and consequently reduced payments to the users.

of TSCM by up to 66% and 34% under M_1 and M_2 modes, respectively.

In Fig. 3 d–f, utility of the crowd-sensing platform is illustrated in the presence of anchor nodes in calculation of user reputation scores, i.e. $i \in A$ in Eqs. 12-13. When compared to Fig. 3 a–c, the deployment of anchor roles in the decentralized component of the collaborative reputation score assessment does not introduce a significant improvement to platform utility. In [21], it was reported that the deployment of anchor nodes would improve platform utility if the anchor population is not less than the malicious user population. However, the reference study employs totally distributed reputation assessment for the participants, which is a vote-based Sybil-detection system. In this paper, based on the results in Fig. 3 a–c and Fig. 3 d–f, we show that the inclusion of a centralized reputation component ($R_i^{stat}(t)$ in Eq. 16, which keeps track of the usefulness of the data through statistical reputation calculation) can provide the same level of platform utility and saves the investment for the anchor nodes. The improvement depends on the operation mode (M_1 or M_2), which affects the calculation of the crowd-sensed task values as well as the value of the recruited crowd as formulated in Eq. 17. As seen in Fig. 3 d–f, when $R_i(0) = 0.7$, under a moderate sensing task arrival rate (i.e. 60 sensing tasks per min), using collaborative reputation scores with anchor nodes improves TSCM by 38% and 24% under the M_1 and M_2 modes, respectively.

D. EVALUATION: USER UTILITY

In Fig. 4 a–c, the average user utility per sensing campaign is illustrated under three different initial reputation values, $R_i(0) \in \{0.3, 0.5, 0.7\}$, for the newly joining participants without deploying anchor nodes to obtain the collaborative reputation scores.

As observed in Fig. 4, when collaborative reputation scores are employed instead of TSCM, the user utility is significantly reduced if the value of the recruited crowd ($v^R(W^\tau)$) is calculated through collaborative reputation scores (M_1 mode in Eq. 17). For example, this reduction is between 20%–32% under varying task arrival rates when $R_i(0) = 0.7$. The reduction in user utility is 10%–15% under the same settings in M_2 mode. On the other hand, as shown in Fig. 4 d–f, in the presence of deployed anchors as the trusted entities in the decentralized component, the reduction in user utility varies between 10%–28% under the M_1 mode. Furthermore, under the M_2 mode and lightly arriving sensing tasks (i.e. 20 tasks/min), the user utility can be improved by 1.2% and the reduction after that point is 3.8%–11.6%. Based on these facts, we reach two conclusions

- Using collaborative reputation scores ($R_i^{coll}(t)$ in Eq. 16 in user recruitment reduces user utility when compared to the purely statistical reputation-based user recruitment ($R_i^{stat}(t)$ in Eq. 6). The reason behind this behavior is that the votes for the neighbors (χ_j^i) can be biased, which may result in reduced reputation ($R_i^{voted}(t)$ component of $R_i^{coll}(t)$ in Eq. 16) and consequently reduced payments to users.
- The bias by the decentralized component of the collaborative reputation assessment can be rectified by using collaborative reputation scores only in the winner selection step of the user recruitment and using statistical reputation values while calculating the value of a recruited crowd ($v^R(W^\tau)$) (M_2 mode in Eq. 17).

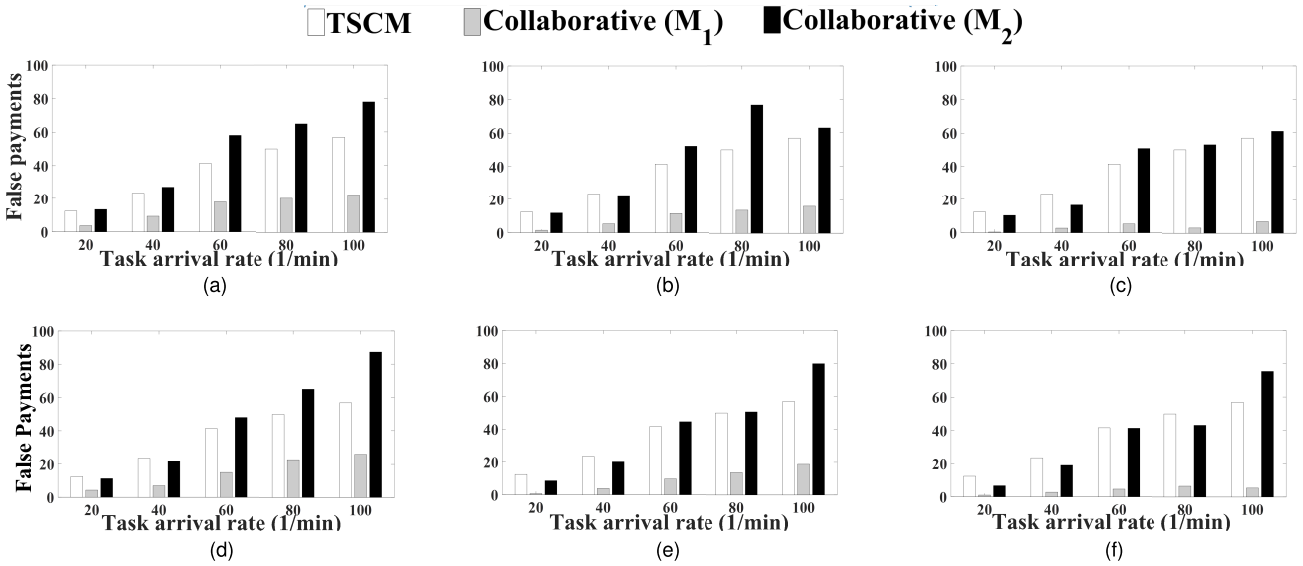


FIGURE 5. False payments (rewards made to malicious users) vs. Sensing Task Arrival Rate. Sub-figures in (a)–(c) depict a deployment **without anchors** with the following initial reputation scores for the newly joining participants: a) $R_i(0) = 0.3$, b) $R_i(0) = 0.5$, c) $R_i(0) = 0.7$. The sub-figures in (d)–(f) depict a deployment **with anchor nodes** with the initial reputation scores d) $R_i(0) = 0.3$, e) $R_i(0) = 0.5$, f) $R_i(0) = 0.7$. Possible user bias in the M_1 mode of the collaborative reputation scores (Eq. 17) works in favor of the MCS platform. When users are recruited based on the collaborative reputation scores ($R_i^{coll}(t)$ in Eq. 16)) and when the value of a recruited crowd is assessed by using those scores (M_1 mode in Eq. 17), the rewards made to the malicious users can be reduced by >90%. In the presence of anchors, using collaborative reputation scores in both modes (M_1 and M_2) can improve the total rewards made to the malicious users until the task arrival rates increase to >100 tasks/min.

E. EVALUATION: TOTAL REWARDS TO MALICIOUS USERS

Total rewards made to malicious users—alternatively defined as *false payments*—is also crucial for platform utility and data trustworthiness. Figure 5 illustrates the results concerning total rewards to malicious users at the end of the crowd-sensing event under different initial reputation values ($R_i(0)$) for the newly joining users.

Here, user bias in the M_1 mode of the collaborative reputation scores (Eq. 17) during the voting phase works in favor of the crowd-sensing platform; when the users are recruited based on the collaborative reputation scores ($R_i^{coll}(t)$ in Eq. 16) and when the value of a recruited crowd is assessed by using those scores (M_1 mode in Eq. 17), the rewards made to the malicious users can be reduced by >90% whereas any compromise from the collaborative reputation (such as in the M_2 mode) may increase the payments made to the malicious users. Furthermore, when anchors are deployed—as shown in Fig. 5 d–f—to assist in the voting phase, using collaborative reputation scores in both modes can improve the total rewards made to the malicious users up to heavy sensing task arrival rates (100 tasks/min).

An overall evaluation of the performance results illustrated and discussed above is presented in Section VI.

VI. CONCLUSIONS

The emergence of cloud computing and Internet of Things (IoT) enables Mobile Crowd-Sensing (MCS) platforms to be formed, in which a community of mobile users use the built-in sensors in their mobile devices—such as gyroscopes, accelerometers, barometers, microphones, cameras, and temperature sensors—to sense several phenomena. One *for-profit* MCS application, Sensing-as-a-Service (S^2aaS), is a promising recipe for the commercialization of the MCS-acquired data by compensating the participants of the MCS community monetarily and selling the data to interested parties. Alternatively, many *not-for-profit* applications exist that formulate the usage of the MCS-acquired data for environmental monitoring and other community-enhancement initiatives.

Whether for commercial use or not, two inter-correlated problems—which are generally studied in conjunction with one another—exist in MCS applications: i) incentivizing the users to participate and ii) ensuring the trustworthiness of the acquired data. While the first challenge can be addressed with proper recruitment schemes, the second one requires the association of a reputation score to each mobile user to quantify the trustworthiness of their acquired data. Data trustworthiness is a non-trivial challenge in MCS systems, because adversaries may lead to disinformation at the service requester site through the manipulation of sensor readings; worse yet, a payment is made to them for the incorrect information they provide. In this paper, we use three metrics, *platform utility*, *user utility*, and *false payments* (the payments to malicious users), that quantify the inter-play between issues (i) and (ii). The goal of a successful MCS system is to maximize *platform utility* by compensating the users sufficiently, which will keep the *user utility* at an acceptable minimum. The third metric—*false payments*—must be minimized to avoid paying for bad information.

In this paper, we present a detailed MCS performance study, centered around these three metrics under multiple user recruitment policies. All of the schemes adopt a reverse auction-based user recruitment procedure but differ in their trustworthiness assurance methods. Among these, TSCM runs a statistical reputation-based method, which keeps track of true and false readings through outlier detection techniques. A decentralized solution, Social Network-Assisted Trustworthiness Assurance (SONATA), uses both statistical and vote-based reputation scores. The third scheme uses collaborative reputation score-based trustworthiness. The study has also been extended to the case where anchor nodes, which are known to be the trusted entities, are used in the decentralized component of collaborative reputation scores. Our simulation results highlight the following results:

- Using collaborative reputation scores in user recruitment improves platform utility and data trustworthiness by reducing false payments (rewards to malicious users).
- Deployment of anchor nodes to assist in the decentralized (i.e., vote-based) component of collaborative reputation scores helps in reducing the false payments, however there is no clearly-evident advantage to use anchor nodes when user reputation scores are collaboratively calculated. Previous studies show an improved platform utility under certain circumstances when the user reputation scores are calculated in a fully decentralized fashion.
- When collaborative methods are employed, using statistical reputation in the assessment of the value of a recruited crowd can reduce the user bias in the decentralized vote-based component of the reputation score; consequently, it can help reduce the negative impact on user utility.
- Our evaluation of the initial reputation of the newly-joining users shows that setting the initial reputation to a value of ≈ 0.3 leads to the most feasible results in terms of platform utility, user utility and data trustworthiness.

We are currently working on incorporating mobility models as well as inter-participant interaction in an MCS platform. As the aim of this paper is laying the foundations of quantifying user reputation in crowdsensing systems, performance study has been limited to simulation results. However, we are currently working on integrating the methods that are presented here with a small-scale crowdsensing testbed to run tests with real multi-dimensional data.

REFERENCES

[1] B. Guo, C. Chen, D. Zhang, Z. Yu, and A. Chin, "Mobile crowd sensing and computing: When participatory sensing meets participatory social media," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 131–137, Feb. 2016.

[2] X. Bao and R. R. Choudhury, "Movi: Mobile phone based video highlights via collaborative sensing," in *Proc. 8th Int. Conf. Mobile Syst. Appl. Services*, 2010, pp. 357–370.

[3] N. D. Lane, S. B. Eisenman, M. Musolesi, E. Miluzzo, and A. T. Campbell, "Urban sensing systems: Opportunistic or participatory?" in *Proc. 9th Workshop Mobile Comput. Syst. Appl.*, 2008, pp. 11–16.

[4] A. T. Campbell *et al.*, "The rise of people-centric sensing," *IEEE Internet Comput.*, vol. 12, no. 4, pp. 12–21, Jul./Aug. 2008.

[5] A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson, "People-centric urban sensing," in *Proc. 2nd Annu. Int. Workshop Wireless Internet*, 2006, Art. no. 18.

[6] Creekwatch Project. *Creekwatch Research Labs by IBM*. 2016. [Online]. Available: http://creekwatch.researchlabs.ibm.com

[7] T. Soyata, *Enabling Real-Time Mobile Cloud Computing through Emerging Technologies*. Hershey, PA, USA: IGI Global, Aug. 2015.

[8] X. Sheng, J. Tang, X. Xiao, and G. Xue, "Sensing as a service: Challenges, solutions and future directions," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3733–3741, Oct. 2013.

[9] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: Current state and future challenges," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 32–39, Nov. 2011.

[10] M. Pouryazdan, C. Fiandrino, B. Kantarci, D. Kliazovich, T. Soyata, and P. Bouvry, "Game-theoretic recruitment of sensing service providers for trustworthy cloud-centric Internet-of-Things (IoT) applications," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Washington, DC, USA, 2016, pp. 1–6.

[11] L. Liu, W. Wei, D. Zhao, and H. Ma, "Urban resolution: New metric for measuring the quality of urban sensing," *IEEE Trans. Mobile Comput.*, vol. 14, no. 12, pp. 2560–2575, Dec. 2015.

[12] B. Guo, H. Chen, Q. Han, Z. Yu, D. Zhang, and Y. Wang, "Worker-contributed data utility measurement for visual crowdsensing systems," *IEEE Trans. Mobile Comput.*, to be published, doi: 10.1109/TMC.2016.2620980.

[13] L. G. Jaimes, I. J. Vergara-Laurens, and A. Raij, "A survey of incentive techniques for mobile crowd sensing," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 370–380, Oct. 2015.

[14] H. Jin, L. Su, D. Chen, K. Nahrstedt, and J. Xu, "Quality of information aware incentive mechanisms for mobile crowd sensing systems," in *Proc. 16th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2015, pp. 167–176.

[15] J.-S. Lee and B. Hoh, "Dynamic pricing incentive for participatory sensing," *Pervasive Mobile Comput.*, vol. 6, no. 6, pp. 693–708, 2010.

[16] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," vol. 24, no. 3, pp. 1732–1744, Jun. 2016.

[17] K. Han, E. A. Graham, D. Vassallo, and D. Estrin, "Enhancing motivation in a mobile participatory sensing project through gaming," in *Proc. IEEE 3rd Int. Conf. Privacy, Secur. Risk Trust*, Oct. 2011, pp. 1443–1448.

[18] P. Bellavista, A. Corradi, L. Foschini, and R. Ianniello, "Scalable and cost-effective assignment of mobile crowdsensing tasks based on profiling trends and prediction: The participact living lab experience," *Sensors*, vol. 15, no. 8, pp. 18613–18640, 2015.

[19] B. Kantarci, P. M. Glasser, and L. Foschini, "Crowdsensing with social network-aided collaborative trust scores," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[20] B. Kantarci, K. G. Carr, and C. D. Pearsall, "SONATA: Social network assisted trustworthiness assurance in smart city crowdsensing," *Int. J. Distrib. Syst. Technol.*, vol. 7, no. 1, pp. 59–78, Jan./Mar. 2016.

[21] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, "Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing," *IEEE Access*, vol. 4, pp. 529–541, 2016.

[22] Gartner. (2016). *Connected Things in Smart Cities*. [Online]. Available: http://www.gartner.com/newsroom/id/3175418

[23] A. D. Cartier, D. H. Lee, B. Kantarci, and L. Foschini, "IoT-big data software ecosystems for smart cities sensing: Challenges, open issues, and emerging solutions," in *Proc. 4th Int. Workshop Cloud IoT (CLIoT)*, 2016, p. 15.

[24] A. Page, T. Soyata, J. P. Couderc, M. Aktas, B. Kantarci, and S. Andreescu, "Visualization of health monitoring data acquired from distributed sensors for multiple patients," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–7.

[25] M. Hassanalieragh *et al.*, "Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges," in *Proc. IEEE Int. Conf. Services Comput. (SCC)*, New York, NY, USA, Jun. 2015, pp. 285–292.

[26] O. Kocabas, T. Soyata, and M. K. Aktas, "Emerging security mechanisms for medical cyber physical systems," *IEEE/ACM Trans. Comput. Biol. Bioinf. (TCBB)*, vol. 13, no. 3, pp. 401–416, Jun. 2016.

[27] A. Page, S. Hijazi, D. Askan, B. Kantarci, and T. Soyata, "Research directions in cloud-based decision support systems for health monitoring using Internet-of-Things driven data acquisition," *Int. J. Services Comput.*, vol. 4, no. 4, pp. 18–34, 2016.
[28] S. Hijazi, A. Page, B. Kantarci, and T. Soyata, "Machine learning in cardiac health monitoring and decision support," *IEEE Comput. Mag.*, vol. 49, no. 11, pp. 38–48, Nov. 2016.
[29] G. Honan, A. Page, O. Kocabas, T. Soyata, and B. Kantarci, "Internet-of-everything oriented implementation of secure digital health (D-health) systems," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Messina, Italy, Jun. 2016, pp. 718–725.
[30] T. Soyata, R. Muraleedharan, C. Funai, M. Kwon, and W. Heinzelman, "Cloud-vision: Real-time face recognition using a mobile-cloudlet-cloud acceleration architecture," in *Proc. 17th IEEE Symp. Comput. Commun. (ISCC)*, Cappadocia, Turkey, Jul. 2012, pp. 59–66.
[31] T. Soyata, H. Ba, W. Heinzelman, M. Kwon, and J. Shi, "Accelerating mobile cloud computing: A survey," in *Communication Infrastructures for Cloud Computing*, H. T. Mouftah and B. Kantarci, Eds. Hershey, PA, USA: IGI Global, Sep. 2013, ch. 8, pp. 175–197.
[32] N. Powers and T. Soyata, "AXaaS (acceleration as a service): Can the telecom service provider rent a cloudlet?" in *Proc. 4th IEEE Int. Conf. Cloud Netw. (CNET)*, Niagara Falls, NY, USA, Oct. 2015, pp. 232–238.
[33] E. Korpela, D. Werthimer, D. Anderson, J. Cobb, and M. Lebofsky, "SETI @HOME: Massively distributed computing for SETI," *Comput. Sci. Eng.*, vol. 3, no. 1, pp. 78–83, 2001.
[34] Gartner. *Worldwide Sales of Wearables*. 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3198018
[35] W. Khan, Y. Xiang, M. Aalsalem, and Q. Arshad, "Mobile phone sensing systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 402–427, 1st. Quart., 2013.
[36] M. Hassanalieragh, T. Soyata, A. Nadeau, and G. Sharma, "Solar-supercapacitor harvesting system design for energy-aware applications," in *Proc. IEEE Int. Syst.-Chip Conf. (SOCC)*, Las Vegas, NV, USA, Sep. 2014, pp. 280–285.
[37] M. Hassanalieragh, T. Soyata, A. Nadeau, and G. Sharma, "UR-SolarCap: An open source intelligent auto-wakeup solar energy harvesting system for supercapacitor-based energy buffering," *IEEE Access*, vol. 4, pp. 542–557, Mar. 2016.
[38] M. Zhu, M. Hassanalieragh, A. Fahad, Z. Chen, T. Soyata, and K. Shen, "Supercapacitor energy buffering for self-sustainable, continuous sensing systems," Dept. Comput. Sci., Univ. Rochester, Rochester, NY, USA, Tech. Rep., TR–995, Mar. 2016.
[39] Open Collaborative Research project involving IBM Research. *Crowd Architecture*. 2016. [Online]. Available: http://researcher.watson.ibm.com/researcher/view_group.php?id=3011
[40] Google Inc. *Science Journal*. 2016. [Online]. Available: https://makingscience.withgoogle.com/science-journal/
[41] D. Zhang, L. Wang, H. Xiong, and B. Guo, "4w1h in mobile crowd sensing," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 42–48, Aug. 2014.
[42] Y. Benazzouz, C. Munilla, O. Günalp, M. Gallissot, and L. Gürgen, "Sharing user IoT devices in the cloud," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 373–374.
[43] W. Tan, M. B. Blake, I. Saleh, and S. Dustdar, "Social-network-sourced big data analytics," *IEEE Internet Comput.*, vol. 17, no. 5, pp. 62–69, May 2013.
[44] B. Guo, Z. Yu, L. Chen, X. Zhou, and X. Ma, "Mobigroup: Enabling lifecycle support to social activity organization and suggestion with mobile crowd sensing," *IEEE Trans. Human-Mach. Syst.*, vol. 46, no. 3, pp. 390–402, Jun. 2016.
[45] K. Hwang and S. Y. Lee, "Environmental audio scene and activity recognition through mobile-based crowdsourcing," *IEEE Trans. Consum. Electron.*, vol. 58, no. 2, pp. 700–705, May 2012.
[46] M. F. Bulut, M. Demirbas, and H. Ferhatosmanoglu, "LineKing: Coffee shop wait-time monitoring using smartphones," *IEEE Trans. Mobile Comput.*, vol. 14, no. 10, pp. 2045–2058, Oct. 2015.
[47] B. Guo, H. Chen, Z. Yu, X. Xie, S. Huangfu, and D. Zhang, "FlierMeet: A mobile crowdsensing system for cross-space public information reposting, tagging, and sharing," *IEEE Trans. Mobile Comput.*, vol. 14, no. 10, pp. 2020–2033, Oct. 2015.
[48] R. Gao *et al.*, "Multi-story indoor floor plan reconstruction via mobile crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1427–1442, Jun. 2016.
[49] C. Zhang, K. P. Subbu, J. Luo, and J. Wu, "GROPING: Geomagnetism and crowdsensing powered indoor navigation," *IEEE Trans. Mobile Comput.*, vol. 14, no. 2, pp. 387–400, Feb. 2015.
[50] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of Things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.
[51] X. Zhang *et al.*, "Incentives for mobile crowd sensing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 54–67, 1st Quart., 2016.
[52] M. Usman, V. Muthukkumarasamy, and X.-W. Wu, "Mobile agent-based cross-layer anomaly detection in smart home sensor networks using fuzzy logic," *IEEE Trans. Consum. Electron.*, vol. 61, no. 2, pp. 197–205, May 2015.
[53] S. Chessa, M. Girolami, L. Foschini, R. Ianniello, A. Corradi, and P. Bellavista, "Mobile crowd sensing management with the particpact living lab," *Pervasive Mobile Comput.*, to be published, doi: 10.1016/j.pmcj.2016.09.005.
[54] T. Soyata, L. Copeland, and W. Heinzelman, "RF energy harvesting for embedded systems: A survey of tradeoffs and methodology," *IEEE Circuits Syst. Mag.*, vol. 16, no. 1, pp. 22–57, 1st Quart., 2016.
[55] A. Fahad, T. Soyata, T. Wang, G. Sharma, W. Heinzelman, and K. Shen, "SOLARCAP: Super capacitor buffering of solar energy for self-sustainable field systems," in *Proc. 25th IEEE Int. Syst.-Chip Conf. (SOCC)*, Niagara Falls, NY, USA, Sep. 2012, pp. 236–241.
[56] G. Honan, N. Gekakis, M. Hassanalieragh, A. Nadeau, G. Sharma, and T. Soyata, "Energy harvesting and buffering for cyber-physical systems: A review," in *Cyber-Physical Systems a Computational Perspective*. Boca Raton, FL, USA: CRC Press, Dec. 2015, ch. 7, pp. 191–218.
[57] S. Reddy, D. Estrin, and M. Srivastava, "Recruitment framework for participatory sensing data collections," in *Proc. 8th Int. Conf. Pervasive Comput.*, May 2010, pp. 138–155.
[58] X. Sheng, J. Tang, and W. Zhang, "Energy-efficient collaborative sensing with mobile phones," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1916–1924.
[59] Y. Chon, Y. Kim, H. Shin, and H. Cha, "Adaptive duty cycling for place-centric mobility monitoring using zero-cost information in smartphone," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1694–1706, Aug. 2014.
[60] H. Xiong, D. Zhang, L. Wang, and H. Chaouchi, "EMC^3: Energy-efficient data transfer in mobile crowdsensing under full coverage constraint," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1355–1368, Jul. 2015.
[61] J. Ren, Y. Zhang, K. Zhang, and X. S. Shen, "SACRM: Social aware crowdsourcing with reputation management in mobile sensing," *Comput. Commun.*, vol. 65, pp. 55–65, Jul. 2015.
[62] R. Pryss, M. Reichert, J. Herrmann, B. Langguth, and W. Schlee, "Mobile crowd sensing in clinical and psychological trials—A case study," in *Proc. IEEE 28th Int. Symp. Comput.-Based Med. Syst.*, Jun. 2015, pp. 23–24.
[63] G. Cardone, A. Cirri, A. Corradi, L. Foschini, and D. Maio, "MSF: An efficient mobile phone sensing framework," *Int. J. Distrib. Sensor Netw.*, to be published, doi: 10.1155/2013/538937.
[64] G. Cardone, A. Cirri, A. Corradi, L. Foschini, R. Ianniello, and R. Montanari, "Crowdsensing in urban areas for city-scale mass gathering management: Geofencing and activity recognition," *IEEE Sensors J.*, vol. 14, no. 12, pp. 4185–4195, Dec. 2014.
[65] F. J. Villanueva, D. Villa, M. J. Santofimia, J. Barba, and J. C. López, "Crowdsensing smart city parking monitoring," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 751–756.
[66] R. Szabo *et al.*, "Framework for smart city applications based on participatory sensing," in *Proc. IEEE 4th Int. Conf. Cognit. Infocommun. (CogInfoCom)*, Dec. 2013, pp. 295–300.
[67] X. Hu, T. H. S. Chu, H. C. B. Chan, and V. C. M. Leung, "Vita: A crowdsensing-oriented mobile cyber-physical system," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 148–165, Jun. 2013.
[68] C. Chowdhury and S. Roy, "Mobile crowdsensing for smart cities," in *Smart Cities Foundations, Principles, and Applications*, H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke, Eds. Hoboken, NJ, USA: Wiley, 2017, ch. 5.
[69] F. Saremi *et al.*, "Experiences with GreenGPS—Efficient navigation using participatory sensing," *IEEE Trans. Mobile Comput.*, vol. 15, no. 3, pp. 672–689, Mar. 2016.
[70] Y. He and Y. Li, "Physical activity recognition utilizing the built-in kinematic sensors of a smartphone," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 4, p. 481580, 2013.
[71] D. He, S. Chan, and M. Guizani, "User privacy and data trustworthiness in mobile crowd sensing," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 28–34, Feb. 2015.

[72] K. L. Huang, S. S. Kanhere, and W. Hu, "Are you contributing trustworthy data?: The case for a reputation system in participatory sensing," in *Proc. 13th ACM Int. Conf. Modeling, Anal., Simulation Wireless Mobile Syst.*, 2010, pp. 14–22.
[73] X. Zhang, Z. Yang, C. Wu, W. Sun, Y. Liu, and K. Liu, "Robust trajectory estimation for crowdsourcing-based mobile applications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1876–1885, Jul. 2014.
[74] B. Kantarci and H. T. Mouftah, "Trustworthy sensing for public safety in cloud-centric Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 360–368, Aug. 2014.
[75] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing," in *Proc. 18th Annu. Int. Conf. Mobile Comput. Netw.*, 2012, pp. 173–184.
[76] M. Pouryazdan and B. Kantarci, "The smart citizen factor in trustworthy smart city crowdsensing," *IEEE IT Prof.*, vol. 18, no. 4, pp. 26–33, Jul. 2016.
[77] Z. Yang, J. Xue, X. Yang, X. Wang, and Y. Dai, "VoteTrust: Leveraging friend invitation graph to defend against social network sybils," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 4, pp. 488–501, Jul. 2016.
[78] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 2, pp. 159–170, 2nd Quart., 2010.
[79] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1732–1744, Jun. 2016.



MARYAM POURYAZDAN (S'16) received the B.Sc. degree in computer engineering from the University of Kerman-Iran in 2011 and the M.Sc. degree in computer science from UTM-Malaysia in 2013. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY. Her research is on trustworthiness assurance in crowd-sensing via mobile social networks.



BURAK KANTARCI (S'05–M'09–SM'12) received the M.Sc. and Ph.D. degrees in computer engineering from Istanbul Technical University, in 2005 and 2009, respectively. From 2014 to 2016, he was an Assistant Professor with the ECE Department, Clarkson University, where he currently holds a courtesy appointment as an Assistant Professor. He was a Visiting Scholar with the University of Ottawa, where he completed the major content of his thesis. He is currently an Assistant Professor with the School of Electrical Engineering and Computer Science, University of Ottawa. He has co-authored over 100 papers in established journals and conferences, and contributed to 11 book chapters. He is a member of the ACM. He received the Siemens Excellence Award in 2005 for his studies in optical burst switching. He also serves as the Secretary of the IEEE ComSoc Communication Systems Integration and Modeling Technical Committee. He is an Editor of the IEEE Communications Surveys and Tutorials and an Area Editor of the IEEE Transactions on Green Communications and Networking.



TOLGA SOYATA (M'08–SM'16) received the B.S. degree in electrical and communications engineering from Istanbul Technical University in 1988, the M.S. degree in electrical and computer engineering from Johns Hopkins University in 1992, and the Ph.D. degree in electrical and computer engineering from the University of Rochester in 2000. He joined the ECE Department, University of Rochester, in 2008. He was an Assistant Professor – Research with UR ECE. In 2016, he joined the Department of ECE, University at Albany, Albany, as an Associate Professor. His teaching interests include CMOS VLSI ASIC design, FPGA-based high performance data processing system design, and GPU architecture, and parallel programming. His research interests include cyber physical systems, digital health, and GPU-based high performance computing. He is a senior member ACM.



LUCA FOSCHINI (S'04–M'08) received the Ph.D. degree in computer science engineering from the University of Bologna, Italy, in 2007. He is currently an Associate Professor with the Department of Computer Science and Engineering, University of Bologna. His interests include distributed systems for pervasive computing environments, system and service management, and cloud computing. He is member of the ACM.



HOUBING SONG (M'12–SM'14) received the Ph.D. degree in electrical engineering from the university of Virginia, Charlottesville, VA, in 2012. In 2012, he joined the Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV, where he is currently the Golden Bear Scholar, an Assistant Professor and the Founding Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us), and the West Virginia Center of Excellence for Cyber-Physical Systems sponsored by West Virginia Higher Education Policy Commission. In 2007, he was an Engineering Research Associate with the Texas A&M Transportation Institute. He is the Editor of four books, including *Smart Cities: Foundations, Principles and Applications* (Hoboken, NJ: Wiley, 2017), *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications* (Chichester, UK: Wiley, 2017), *Cyber-Physical Systems: Foundations, Principles and Applications*, (Waltham, MA: Elsevier, 2016), and *Industrial Internet of Things: Cybermanufacturing Systems* (Cham, Switzerland: Springer, 2016). He has authored over 100 articles. His research interests include cyber-physical systems, Internet of Things, cloud computing, big data analytics, connected vehicle, wireless communications and networking, and optical communications and networking. He is a member of the ACM. He was a very first recipient of the Golden Bear Scholar Award, the highest faculty research award at the West Virginia University Institute of Technology (WVU Tech), in 2016.