Mobility-aware Trustworthy Crowdsourcing in Cloud-Centric Internet of Things

Burak Kantarci, *Senior Member, IEEE,* and Hussein T. Mouftah, *Fellow, IEEE*

***Abstract*—In the Internet of Things (IoT) era, smart devices that are equipped with various types of sensors can enable access to the IoT architecture through a cloud-inspired service model, namely Sensing-as-a-Service (S^2aaS). S^2aaS can provide crowdsourced data to an application running on a cloud platform. The crowdsourced data can be used for several purposes such as public safety. One of the biggest challenges here is the incentive mechanisms for the users who are requested to provide S^2aaS. In this paper, we propose mobility-aware trustworthy crowdsourcing (MATCS) framework in a cloud-centric IoT architecture which adopts and extends a previous scheme, Trustworthy Sensing for Crowd Management (TSCM) [1] by incorporating user mobility-awareness in the presence of maliciously altered sensing data. MATCS employs a user-centric incentive mechanism which collects sensing data based on an auction procedure. In the auction procedure, MATCS uses users' reputations, bids, current location and their estimated dislocation during crowdsourcing process. Furthermore, in order to investigate the benefits of reputation-awareness, we also propose reputation-unaware Mobility-Aware Crowdsourcing (MACS). Performance of MATCS is evaluated via simulations, and it is compared to MACS and a benchmark scheme, which aims at making a compromise between the utilities of the users and the platform by considering neither mobility nor trustworthiness. Simulation results confirm that mobility-awareness improves the utility of the platform significantly whereas combining reputation-awareness and mobility-awareness by MATCS can triple the improvement. Besides, user incomes are not significantly impacted by MACS or MATCS when users are mobile. Furthermore, maliciously altered data ratio can be degraded by 20%$\sim$55% by reputation-awareness in MATCS.**

***Index Terms*—Auction theory; cloud computing; crowd management; public safety, Sensing-as-a-Service (S^2aaS); smart phone sensing.**

I. Introduction

Future Internet which is expected to be dominated by cloud computing paradigm by providing everything-as-a-service (XaaS) can enable access to the Internet of Things (IoT) architecture where billions of embedded devices are uniquely identified and inter-connected [2]. As a part of the cloud-centric IoT, Sensing-as-a-Service (S^2aaS) enables collecting sensed data through numerous smart devices equipped with various types of sensors based on pay-as-you-go fashion [3].

Since sensing objects require huge computing and storage capacity, real-time processing of big data, scalable on-demand access to the IT resources, proper web interfaces and security/privacy assurance, integration of cloud computing in the IoT framework is inevitable [4]. Furthermore, sending the data sensed by the built-in sensors in mobile devices to cloud servers introduces significant savings in communication overhead and energy [5]. Application areas of S^2aaS in Cloud-centric IoT are various such as healthcare, weather forecast, road monitoring. In this paper, we focus on addressing public safety in smart city management through cloud-centric IoT [6]. In such an architecture, mobile users require effective incentives in order to be willing to offer S^2aaS to the customers/authorities/individuals who request crowdsourced sensing data of various tasks [3].

In this paper, we propose Mobility-Aware Crowdsourcing (MACS) framework in a cloud-centric IoT architecture providing S^2aaS to a smart city management platform for public safety. MACS uses a user-centric incentive mechanism which selects the users based on an auction and make payments to the selected users based on their bids and the platform utility. While selecting the winners of an auction, MACS forecasts the future location of the users participating the auction, and excludes the ones who are forecasted to be out of the range of any sensing tasks until the end of the ongoing auction. In such a public safety scenario, it is very likely to have malicious users who send altered data to the cloud platform by aiming at disinformation at the smart city management authority. In order to address this challenge, we enhance MACS by incorporating reputation-awareness, and call this alternate scheme Mobility-Aware Trustworthy Crowdsourcing (MATCS). MATCS adopts reputation-awareness in our previously proposed scheme, Trustworthy Sensing for Crowd Management (TSCM) in [1].

Smart city management authority requests sensing data from smart phone users who are willing to participate crowdsourcing through an auction. The users participate the auction by sending their bids to sense a particular phenomenon which is within their area of interest. Smart city management authority uses users' reputations in order to reduce disinformation due to maliciously altered data. Furthermore, it uses estimated location of the users prior to selecting the winners of the auction and making payments to the winners. Based on the truthfulness of the data received from each user, user trustworthiness values are updated. Besides their estimated location and trustworthiness, smart city management authority also uses the marginal value of each sensed data and bids of the users to select winners and determine payments. We evaluate the mobility-aware crowdsourcing framework via simulations. Simulation results show that MACS improves the utility of the management authority significantly when compared to the case under the mobility-unaware auction. Furthermore, employment of MTACS triples the utility of the management authority as a result of incorporating reputation-awareness. Besides, we show that mobility-awareness incorporated with reputation-awareness can reduce disinformation probability by 20%$\sim$55%.

The paper is organized as follows. In Section II, related

B. Kantarci and H. T. Mouftah are with the School of Electrical Engineering and Computer Science of the University of Ottawa, Ottawa, ON, K1N 6N5, Canada. e-mail: {kantarci,mouftah}@site.uottawa.ca

work and motivation are presented while Section III presents the proposed frameworks MACS and MATCS in detail. Numerical results are presented and discussed in Section IV while Section V concludes the paper and gives future directions.

II. Related Work and Motivation

The Cloud is defined as a front-end access to the IoT architecture which requires massive processing power and storage capacity. A previous study defines S^{2}aaS as a four-layer business model in the IoT architecture which is formed by users and sensors, sensing data publishers, cloud service providers and S^{2}aaS [7]. This definition also forms a basis to our proposed framework, as well.

This architecture faces several challenges including location of the users (i.e., built-in sensors), residual battery power, reliability and so on. The authors in [8] address this problem through a context-aware ranking scheme for the sensing devices. Another important challenge is the definition of effective incentives which is reported along with a comprehensive survey on S^{2}aaS cloud in [3].

In [9], the authors define two types of incentives, namely user-centric and platform centric approaches. User-centric incentives assume knowing users who aim at participating crowdsourcing activities whereas platform-centric incentives select users for a crowdsourcing task and allow each user to run its own sensing plan. As mentioned in [1], as smart phones are expected to be more widely used, users will get more willing to provide their sensing data as a service to the cloud customers based on the pay-as-you-go-fashion. Therefore, in this paper, we consider user-centric incentives where the cloud platform determines the users who will provide S^{2}aaS and their corresponding payments through an auction.

In [9], the authors propose an effective user-centric incentive, namely MSensing which maximizes the utility of the cloud platform while ensuring truthful bidding of the users. Thus, malicious users who aim at increasing their incomes by participating the auction with higher bids are detected and not selected by employing a monotonously increasing selection approach in the auction. In [1], MSensing has been enhanced to address the issues which may occur in the presence of malicious users who aim at disinformation. To this end, we have proposed a reputation-aware S^{2}aaS scheme for crowdsourcing in public safety, namely Trustworthy Sensing for Crowd Management (TSCM) which uses user trustworthiness in the auction (both user selection and payment decisions) and dynamically adjusts the user trustworthiness values based on the accuracy of their sensing data.

In a public safety application, user mobility is a big challenge which may affect the platform utility. Moreover the existence of users aiming at disinformation can further reduce platform utility while increasing disinformation probability at the public safety authority. Therefore, the motivation behind this study is two-fold: 1) The impact of mobility in a public safety scenario needs to be addressed, 2) A new user-centric incentive which combines mobility-awareness and trustworthiness is needed in order to maximize the utility of the public safety authority and minimize disinformation probability.

III. Mobility-Aware and Trustworthy S^{2}aaS

A. System architecture

As summarized in [1], the system architecture consists of four layers. The first layer is the smart city management authority which is a cloud customer, and it interacts with the cloud computing platform which is formed by hosts, sensing servers, user/sensing-data databases and web servers. Computation and storage is done in the cloud computing platform whereas publishing sensing data requires an additional layer. As most smart phones have social networking applications installed and enabled access to the data stored in the smart phone, those applications can aide publishing sensing data, as well as retrieving users locations who are (or will be) within the vicinity of a group of sensing tasks. Besides, social networking applications have been pointed as useful enablers in previous studies [10] whereas integration of IoT and social networks requires more investigation [11]. Although it is not mandatory, our framework also considers data publishing layer utilizing social networking applications. Fourth layer is the users who take part the crowdsourcing of sensing tasks in a particular region by participating an auction with their bids.

Crowdsourcing starts with smart city management authority's sending a S^{2}aaS request to the cloud platform regarding a particular region in the city. The S^{2}aaS request consists of the set of tasks and their locations in the corresponding region. Upon receiving the request, the cloud platform interacts with the sensing data publishing layer, queries the user database and retrieves the users who have already checked-in at a location which is within the corresponding region. As it is known, social networking applications enable users to check-in at specific locations. Thus, the cloud platform retrieves the list of users through social networks. Retrieval of the users is followed by updating the user database and publishing the set of tasks and their locations within the corresponding region through social networks visible to the users in the region. Each user replies back with his/her tasks of interest along with the corresponding bids for the tasks. In the next step, the cloud platform runs an auction to select the users who will participate crowdsourcing, and it determines the payments to be made to the selected users. The selected users publish their sensing data over their social network which is visible to the cloud platform. The cloud platform finally, runs an anomaly detection algorithm, detects outliers in the crowdsourced sensing data, updates user reputations in the database, and sends crowdsourced data to the customer, namely the smart city management authority.

B. Auction Mechanism

User selection and payment determination steps call an auction procedure which mainly adopts the MSensing auction in [9]. The auction consists of two steps, namely the winner selection step and payment determination step. Before proceeding with the details of the procedure, it is worthwhile to take a closer look at the definitions used in the auction. We use the notation in Table I:

Given each task t has a pre-defined value, ϑ_t, $\vartheta_i(W)$ stands for the additional value introduced to the set by including the

TABLE I
THE NOTATION USED IN THE FORMULATION

Notation	Explanation
P:	Set of users participating S^2aaS
W:	Set of winners in the auction
$\Re_i(t)$:	Trustworthiness of user-i at time period-t
$\Re_i$:	Overall trustworthiness of user-i
$\vartheta(W)$:	Total value of the sensing tasks handled by the users in the set-W
$\vartheta^{\Re}(W)$:	Reputation-based value of the sensing tasks handled by the users in the set-W
$\vartheta_i^{\Re}(W)$:	Reputable marginal value of the user on the set W
b_i:	Bid of the user-i
c_i:	Cost of the user-i
ρ_i:	Payment to user-i
Ω :	Reputation list
Φ :	Payments list
T :	Set of tasks
T_S :	Set of tasks handled by the users in the set, S
T_i :	Set of tasks handled by user-i
$\overrightarrow{v_i}$:	Velocity of user-i
x_i^t, y_i^t :	Location of user-i at time-t
T_{pause}^i :	Average pause time of user-i
T_{walk}^i :	Average walking time of user-i
ϑ_t:	Value of task-t
Γ_t:	Set of users handling task-t

sensing tasks of user-i in the set, $T_{W\setminus\{i\}}$ where T_W is the set of tasks sensed by the users in W. While selecting the users, MSensing sorts the users based on their marginal values and selects the first W users, the union of whose sensing tasks can cover T, the set of tasks assigned by the platform. Marginal value of a user is formulated in Eq. 1 whereas the value introduced by the users in set-W is denoted by $\vartheta(W)$ and formulated by Eq. 2.

$$\vartheta_i(W) = \vartheta(W \cup \{i\}) - \vartheta(W) \tag{1}$$

$$\vartheta(W) = \sum_{t \in T_W} \vartheta_t \tag{2}$$

In order to determine the payments to the selected users, users are sorted based on their marginal value contributions to the set of sensing tasks. Given that any user will be paid no less than his/her bid, for each user who has not been paid so far, the algorithm aims at finding a bid value which enables preferring the corresponding user over any other user who has not been paid so far.

C. Mobility-Aware Crowdsourcing (MACS)

In MSensing, mobility of the users is not considered, however in a scenario where smart city management authority aims at obtaining information regarding public safety of a region, mobile phone users passing through the corresponding region can provide S^2aaS by participating the auction. Here, mobility of these users may degrade the utility of the platform since a user that is selected and paid in the auction can possibly wander off the corresponding sensing task by the end of the auction. In order to overcome this issue, we propose Mobility-Aware Crowdsourcing (MACS) based on the following assumptions:

i) Mobile phone users adopt random way-point mobility model [12] on a grid topology representing the region. Thus, at time t, a user at the location (x_i^t, y_i^t) selects a random destination (X, Y) and walks towards the destination with an average velocity of $\overrightarrow{V}$. Once it reaches at the destination, it pauses for the duration of T_{pause}. At the end of T_{pause}, the user selects a new destination (X', Y') and walks towards it with a new velocity $\overrightarrow{V'}$. If the user arrives at a point lying on the boundary of the region, it immediately selects a new destination and walks towards it with a new velocity.

ii. The cloud platform keeps track of the mobility pattern of each user in the database, and makes an estimation on the next location of a user in τ units of time denoted by ($x_i^{t+\tau}$, $y_i^{t+\tau}$).

Estimated location of a user is calculated as follows. By running a lightweight triangulation method [13]. In our formulation (see Eqs. 3-4), ($x_i^{t^-}$,$y_i^{t^-}$) denotes the moving average of previous (x, y) coordinates of the user. Thus, ($x_i^{t^-}$,$y_i^{t^-}$), (x_i^t,y_i^t), and ($x_i^{t+\tau}$,$y_i^{t+\tau}$) are considered to be three points on the hypotenuse of a right triangle whereas the distance between (x_i^t,y_i^t), and ($x_i^{t+\tau}$,$y_i^{t+\tau}$) is calculated by the product of the norm of the velocity vector and the offset time, namely τ.

$$x_i^{t+\tau} = \left\{ \begin{array}{cc} x_i^t + \left\lfloor \frac{x_i \cdot |\overrightarrow{V_i}| \cdot \tau}{\sqrt{(y_i^t - y_i^{t^-})^2 + (x_i^t - x_i^{t^-})^2}} \right\rfloor & x_i^t - x_i^{t^-} \geq 0 \\ x_i^t - \left\lfloor \frac{x_i \cdot |\overrightarrow{V_i}| \cdot \tau}{\sqrt{(y_i^t - y_i^{t^-})^2 + (x_i^t - x_i^{t^-})^2}} \right\rfloor & else \end{array} \right\} \tag{3}$$

$$y_i^{t+\tau} = \left\{ \begin{array}{cc} y_i^t + \left\lfloor \frac{y_i \cdot |\overrightarrow{V_i}| \cdot \tau}{\sqrt{(y_i^t - y_i^{t^-})^2 + (x_i^t - x_i^{t^-})^2}} \right\rfloor & y_i^t - y_i^{t^-} \geq 0 \\ y_i^t - \left\lfloor \frac{y_i \cdot |\overrightarrow{V_i}| \cdot \tau}{\sqrt{(y_i^t - y_i^{t^-})^2 + (x_i^t - x_i^{t^-})^2}} \right\rfloor & else \end{array} \right\} \tag{4}$$

When providing S^2aaS in MACS, the cloud platform computes the estimated next locations of the users by the end of the auction. For each user who has sent his/her bids for the sensing tasks in his/her sensing range, the algorithm recomputes the set of sensing tasks that are expected to be still within his/her range based on his/her estimated location by the end of the auction. Then, MACS calls the conventional MSensing auction which has been briefly summarized above and presented in [9] in detail.

D. Mobility-aware Trustworthy Crowdsourcing (MATCS)

Platform utility is mainly dependent on the utility of malicious users who are aiming at disinformation at the smart city management authority by sending altered sensing data. Therefore, we extend MACS by incorporating trustworthiness which denotes a user's reputation as a function of time ($\Re_j(t)$). We adopt the trustworthiness definition in [1] and formulate its value for the auction at time-t as seen in Eq. 5. Upon receiving each sensor reading, the cloud platform runs an outlier detection algorithm [14]. A sensor reading which is classified as an outlier is tagged as a negative reading (n) whereas a non-outlier sensor reading is tagged as a positive reading (p).

$$\Re_j(t) = \frac{p(t)+1}{p(t)+n(t)+2} \tag{5}$$

As the trustworthiness of a user may vary by time, instantaneous reputation should be used to obtain the trustworthiness of the user which is stored and updated in the database in the cloud platform. As formulated in Eq. 6, weighted sum of previous and current reputations of a user are used to obtain the trustworthiness. The weight, α_j, is adaptively modified based on the relation between positive and negative readings of user-j as seen in Eq. 7. Thus, at time-t, if positive readings of user-j are less than negative readings of the corresponding user, α_j is decremented by α_{step} increasing the impact of past reputations as shown in Eq. 7. Similarly, if positive readings of user-j are greater than or equal to negative readings of the corresponding user, α_j is incremented by α_{step} increasing the impact of current reputation.

$$\Re_j = \alpha_j \cdot \Re_j(t) + (1-\alpha_j) \cdot \Re_j^- \tag{6}$$

$$\alpha_j = \left\{ \begin{array}{cc} max(\alpha_j - \alpha_{step}, \alpha_{min}) & p_j(t) < n_j(t) \\ min(\alpha_J + \alpha_{step}, \alpha_{max}) & else \end{array} \right\} \tag{7}$$

Since MATCS adopts TSCM, while calculating the marginal value contribution of a user to a set, W, it uses the "*adaptive reputable value*" of a set of tasks as shown in Eq. 8. Thus, if the user reputation has increased since last auction, the platform uses the regular marginal value definition in Eq. 1. On the other hand, if the reputation of the user has decreased since last auction, it uses the reputable marginal value contribution to the corresponding set. Reputable value of set-W is the sum of the reputable value of the tasks as formulated in Eq. 9. Reputable value of a task is its absolute value scaled by the average reputation of the users who participate sensing the corresponding task.

$$\vartheta_i^{\Re}(W) = \left\{ \begin{array}{cc} \vartheta^{\Re}(W \cup \{i\}) - \vartheta^{\Re}(W) & if\ \Re_i \leq \Re_i^- \\ \vartheta_i(W) & else \end{array} \right\} \tag{8}$$

$$\vartheta^{\Re}(W) = \sum_{t \in T_W} \sum_{j \in \Gamma_t} \vartheta_t \cdot \Re_j / |\Gamma_t| \tag{9}$$

Similar to MACS, upon receiving the list of users who join the auction to participate sensing a subset of the tasks MATCS computes estimated locations of the participants at the end of the auction. In order to select the winners of the auction, it adopts the methodology in [1], and sorts the users with respect to their reputable marginal values and "*modified bids*". It is worthwhile to note that the modified bid of a user stands for the actual bid of a user scaled by his/her trustworthiness. Thus, the modified bid of user-p is $b_p/\Re_p$. The reason of using the modified bid of a user in the selection process is increasing the selection probability of a user with a lower bid and higher reputation over the other users. The users whose modified bids are less than their reputable marginal values are selected as the winners of the auction and added to the winners list, W in decreasing order. A user with higher *reputable* contribution to the platform's utility is closer to the head of the list and vice versa. Thus, $(\vartheta_i^{\Re} - b_i/\Re_i) > (\vartheta_{i+1}^{\Re} - b_{i+1}/\Re_{i+1})$.

Payment determination phase of MATCS adopts the same method in TSCM [1], as well as MSensing [9], for payment determination. It is ensured that any user, user-w will be paid no less than his/her bid. For each user-w in the winners set, W, the algorithm generates a temporary set, Δ, consisting of user-w_v's whereas user-w_v denotes a user in the set of participants, whose reputable marginal value in Δ is greater than its modified bid. The algorithm sorts Δ with respect to the reputable contributions of the users. Then it searches for maximum possible value for the bid of user-w so that selection of user-w would still be viable instead of user-w_v. Thus, the sorting will look like as in Eq. 10.

$$(\vartheta_{w_v}^{\Re} - b_{w_v}/\Re_{w_v}) > \vartheta_{w_v+1}^{\Re} - b_{w_v+1}/\Re_{w_v+1} \tag{10}$$

Payment determination step sets an upper bound for the runtime of MATCS. In the worst case, number of selected users (W) is equal to the number of users (P) where the algorithm has to go through both loops $\Delta = P'$ and $|P-1|$ times. Besides, for each task $t \in \Delta$, $\Gamma_t = |P-1|$; hence computation of the reputable value of Δ is $O(|P| \cdot T_\Delta)$. Therefore, complexity of the auction is $O(|P|^3 \cdot T_\Delta)$. Since $T_\Delta \ll P$, the complexity of the algorithm is $O(|P|^3)$.

IV. Numerical Results

A. Simulation Settings

We evaluate MACS and MATCS frameworks in a 1000mx1000m region where 1000 users are uniformly distributed at the beginning. Each user is assumed to move based on the random waypoint mobility model. A user randomly selects a destination in the 1000x1000 grid and starts walking towards the destination with a speed of 2 m/s and pauses there for T_{pause} seconds. Then, he/she selects a new destination and starts walking towards the new destination. T_{pause} is uniformly distributed between three to five minutes. 5% of the users are assumed to be in malicious activity aiming at disinformation at the smart city management authority. We assume that the built-in sensors of mobile smart devices have sensing accuracy of 0.97$\sim$0.98 [15]. In each simulation scenario, smart city management authority sends λ task requests per minute to the social networking service where sensing tasks are also uniformly distributed over the terrain. The value of a task is uniformly distributed over $[1, 5]$ while a user bid is uniformly distributed over $[1, 10]$. A user shows interest to a task within his/her 30m range [9]. Each simulation runs for 30 virtual minutes. An auction is assumed to end in five seconds.

Malicious users participate the auction by bidding lower than their cost. Therefore, they aggressively aim at winning in the auction by bidding 0.1 times of their costs. On the other hand, since the platform selects the users based on their trustworthiness, in order to keep his/her reputation at a level which may enable him/her to be re-selected, a malicious user may keep track of his/her activity in order to compute his/her trustworthiness. Thus, he/she sends unaltered sensor readings until he/she ensures that his/her trustworthiness exceeds a threshold, $UP\_THRESHOLD$. At this point, the user starts publishing altered sensing data over his/her social network in order to lead to disinformation at the smart city management authority. As the cloud platform will start degrading the corresponding user's trustworthiness, a malicious user who finds his/her trustworthiness below a threshold, $DOWN\_THRESHOLD$, starts sending truthful sensor readings. These two thresholds are taken as 0.8 and 0.5, respectively.

We use utility of the smart city management authority (i.e., platform utility), average user utility, disinformation probability and total payment to malicious users as our performance metrics. Platform utility is the difference between the total reputable value of the sensing tasks and the total payments made to the winners in the auction as formulated in Eq. 11 where τ denotes the τ^{th} period in which the crowd management authority requests a new set of tasks through the cloud platform. Average user utility is the difference between total payments made to the winners and the total sensing cost of the winners as formulated in Eq. 12. Disinformation Ratio (DIR) is the ratio of the tasks for which at least one malicious user has been paid, to the total number of tasks as formulated in Eq. 13.

$$U_{auth} = \sum_{\tau} \left(\sum_{t \in T_{W_\tau}} \vartheta^{\tau}(W_\tau) - \sum_i {\rho_i}^{\tau} \right) \quad (11)$$

$$U_{user} = \left(\sum_{\tau} \left((\sum_i {\rho_i}^{\tau} - \sum_i {c_i}^{\tau})/|W_\tau| \right) \right) / \tau_{end} \quad (12)$$

$$DIR = \left(\sum_{\tau} (\sum_{t \in T_W^{\tau}} \sum_{i \in \Gamma_t} sgn(\rho_i))/|T_W| \right) / \tau_{end} \quad (13)$$

B. Simulation results

In Fig. 1, we illustrate the utility of the smart city management authority under MACS, MATCS and reputation-and-mobility-unaware sensing. Mobility-awareness of MACS significantly increases the utility of the smart city management authority under heavily arriving sensing task requests whereas enhancement in the utility of the authority is tripled under moderate and lightly arriving sensing task requests. Furthermore, reputation-awareness incorporated with mobility-awareness by MATCS improves the performance of mobility-aware crowdsourcing by approximately 20%. MATCS determines the winners, as well as the payments based on the reputable values of the task sets; hence it is expected to lead to cuts in the payments made to the users with lower reputation.

Fig. 2 illustrates the disinformation ratio (DIR) under the three crowdsourcing schemes. MACS improves the benchmark either under lightly arriving sensing task requests (i.e., 20 tasks /min) or heavily arriving sensing tasks requests (i.e., 100 tasks/min) in terms of DIR. Under moderate light loads its reputation-unaware nature leads to increase in disinformation although mobility-awareness improves platform utility. Since, MSensing is mobility unaware, it is more likely to include non-malicious users as the winners whereas in case of MACS, a wrong estimation in the next location of a non-malicious user may lead to selection of a malicious user instead. As seen in the figure, reputation-and-mobility-awareness improves disinformation ratio by 55% under heavy loads and by 18% under light loads. In fact this is an expected behavior as MATCS avoids occurrence of the situation defined above.

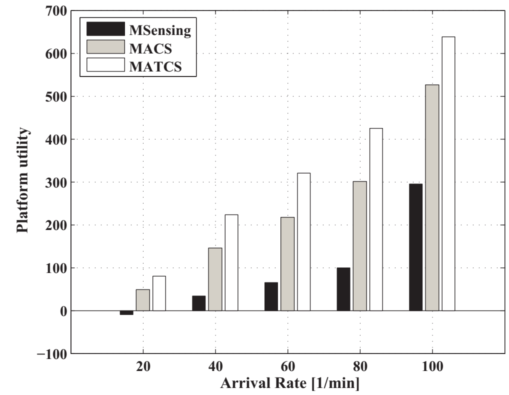

Fig. 1. Utility of the smart city management authority

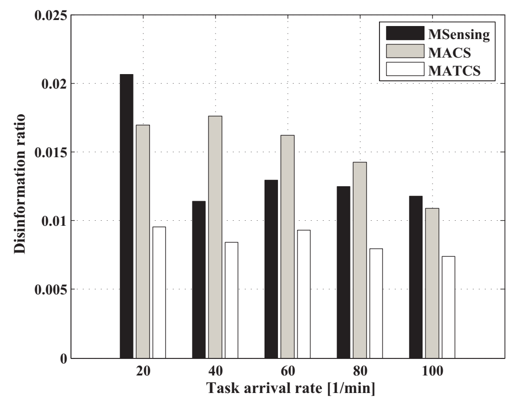

Fig. 2. Average disinformation ratio

In Fig. 3, total payments to the malicious users are shown. The figure complements the results presented in Fig. 2. The behavior of the three schemes in terms of payments made to the malicious users follows the same trend with their behavior in terms of disinformation ratio. Thus, MATCS can achieve around 55% cuts in the incomes of malicious users under heavily arriving sensing task requests.

Fig. 4 shows the average utility of a user participating the auction. Considering the results in Figs. 1-3 along with Fig. 4, the improvement in the utility of the smart city management authority, savings in the payments to the malicious users, and improvement in DIR by MATCS are at the expenses of reduction in user utility. However, when compared the improvement in other performance metrics, the reduction in

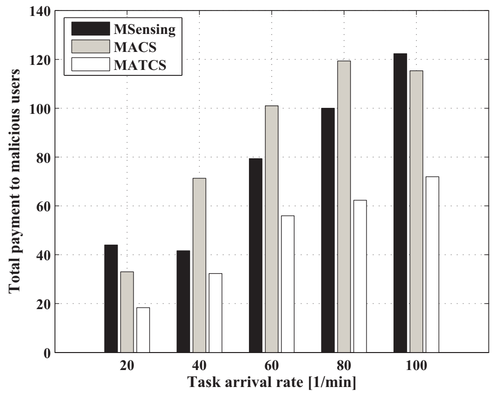

Fig. 3. Total payment to malicious users

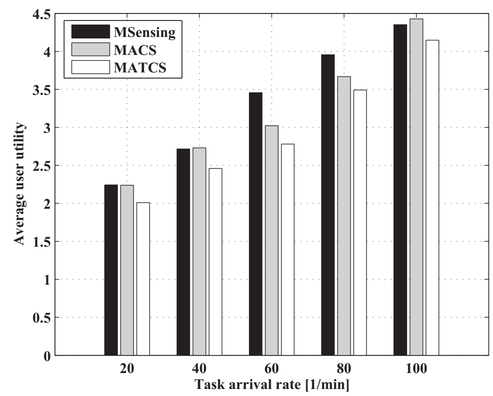

Fig. 4. Average utility of a participant

user utility is significantly low. Furthermore, when sensing task requests arrive more frequently, the degradation in user utility is significantly lower under MATCS. It is worthwhile to note that every selected user is ensured to be paid at least his/her actual cost which is supposedly reported as the bid of the corresponding user. Hence, degradation in user utility is acceptable as MATCS introduces significant enhancement in truthfulness of the sensing data and utility of the smart city management authority.

V. Conclusion

We have proposed a mobility and reputation-aware framework for a cloud centric IoT architecture with the aim of smart city management over social networking services, namely Mobility-Aware Trustworthy Crowdsourcing (MATCS). In MATCS, the cloud platform confirms the presence of the participants who are willing to collaborate with the smart city management authority by publishing their sensing data and bids over their social networks. The cloud interacts with the public safety authority, social networking services and the participants in order to match the users with arriving sensing tasks based on an auction. The cloud platform periodically updates the trustworthiness of users, which are used in assigning sensing tasks to the users. Moreover, payments made to the winners of the auction are determined based on the bids, marginal values as well as the trustworthiness of the corresponding users. Furthermore, the cloud platform estimates the expected location of a mobile user by the end of the auction so that a user who is expected to be out of range of a sensing task will not be paid. MATCS also aims at preventing disinformation caused by maliciously altered sensing data and thereupon improving the utility of the authority. We have evaluated the performance of MATCS through simulations and have shown that incorporation of user mobility-awareness and reputation-awareness in crowdsourcing, utility of the smart city management authority can be improved significantly (up to 70%), and the disinformation probability can be degraded by up to 55%. Furthermore, the payments made to the malicious users who aim at disinformation at the smart city management authority can be reduced by the same ratio.

References

[1] B. Kantarci and H. T. Mouftah, “Reputation-based Sensing-as-a-Service for Crowd Management Over the Cloud,” in *IEEE Intl. Conf. on Communications (ICC)*, June (accepted) 2014.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

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

[4] Zhou J., T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, H. Jin, and L.T. Yang, “CloudThings: A common architecture for integrating the Internet of Things with cloud computing,” in *IEEE 17th Intl. Conf. on Computer Supported Cooperative Work in Design (CSCWD)*, June 2013, pp. 651–657.

[5] C. Perera, P. Jayaraman, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Dynamic configuration of sensors using mobile sensor hub in Internet of Things paradigm,” in *IEEE Eighth Intl. Conf. on Intelligent Sensors, Sensor Networks and Information Processing*, Apr. 2013, pp. 473–478.

[6] W. Li, J. Chao, and Z. Ping, “Security structure study of city management platform based on cloud computing under the conception of smart city,” in *Fourth Intl. Conf. on Multimedia Information Networking and Security (MINES)*, Nov. 2012, pp. 91–94.

[7] . Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Sensing as a service model for smart cities supported by Internet of Things,” *Transactions on Emerging Telecommunications Technologies*, (accepted) 2014.

[8] C. Perera, A. Zaslavsky, C. Liu, M. Compton, P. Christen, and D. Georgakopoulos, “Sensor search techniques for Sensing as a Service Architecture for The Internet of Things,” *IEEE Sensors Journal*, vol. PP, no. 99, pp. 1–1, 2013.

[9] D. Yang, G. Xue, X. Fang, and J. Tang, “Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing,” in *18th Intl Conf. on Mobile Computing and Networking (Mobicom)*, Aug. 2012, pp. 173–184.

[10] Y. S. Yilmaz, M. F. Bulut, C. G. Akcora, M. A. Bayir, and M. Demirbas, “Trend sensing via twitter,” *Int. Journal of Ad Hoc and Ubiquitous Computing*, vol. 14, no. 1, pp. 16–26, 2013.

[11] L. Atzori, A. Iera, and G. Morabito, “SIoT: Giving a social structure to the Internet of Things,” *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, Nov 2011.

[12] T. Camp, J. Boleng, and V. Davies, “A survey of mobility models for ad hoc network research,” *Wireless Communications and Mobile Computing*, vol. 2/5, pp. 483–502, 2002.

[13] M. Kim, D. Kotz, and S. Kim, “Extracting a mobility model from real user traces,” in *25th IEEE Intl. Conf. on Computer Communications (INFOCOM)*, 2006, pp. 1–13.

[14] Y. Zhang, N. Meratnia, and P. Havinga, “Outlier Detection Techniques for Wireless Sensor Networks: A Survey,” *IEEE Communications Surveys Tutorials*, vol. 12, no. 2, pp. 159–170, 2nd Quarter 2010.

[15] Y. He and Y. Li, “Physical activity recognition utilizing the built-in kinematic sensors of a smartphone,” *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.