Game-Theoretic Recruitment of Sensing Service Providers for Trustworthy Cloud-Centric Internet-of-Things (IoT) Applications

Maryam Pouryazdan[†], Claudio Fiandrino[⋆], Burak Kantarci[±†], Dzmitry Kliazovich[⋆], Tolga Soyata[‡], Pascal Bouvry[⋆]

[†] Department of Electrical and Computer Engineering, Clarkson University, NY, USA

[⋆] Computer Science and Communications Research Unit, University of Luxembourg, Luxembourg

[±] School of Electrical Enginering and Computer Science, University of Ottawa, ON, Canada

[‡] Department of Computer Engineering, State University of New York (SUNY) at Albany, NY, USA

E-mails: [†] pouryam@clarkson.edu, [⋆]{firstname.lastname}@uni.lu, [±] burak.kantarci@uOttawa.ca [‡] tsoyata@albany.edu

***Abstract*—Widespread use of connected smart devices that are equipped with various built-in sensors has introduced the mobile crowdsensing concept to the IoT-driven information and communication applications. Mobile crowdsensing requires implicit collaboration between the crowdsourcer/recruiter platforms and users. Additionally, users need to be incentivized by the crowdsensing platform because each party aims to maximize their utility. Due to the participatory nature of data collection, trustworthiness and truthfulness pose a grand challenge in crowdsensing systems in the presence of malicious users, who either aim to manipulate sensed data or collaborate unfaithfully with the motivation of maximizing their income. In this paper, we propose a game-theoretic approach for trustworthiness-driven user recruitment in mobile crowdsensing systems that consists of three phases: i) user recruitment, ii) collaborative decision making on trust scores, and iii) badge rewarding. Our proposed framework incentivizes the users through a sub-game perfect equilibrium (SPE) and gamification techniques. Through simulations, we show that the platform and user utilities, defined in terms of costs and revenues, can be improved respectively by up to the order of 50% and of at least 15% when compared to fully-distributed and user-centric trustworthy crowdsensing.**

***Index Terms*—Crowdsensing, gamification, subgame perfect equilibrium (SPE), reputation systems, user incentives**

I. Introduction

Mobile crowdsensing (MCS) has become an emerging paradigm for large-scale distributed sensing that requires an implicit collaboration between crowdsensing platforms and participants who provide sensed data as a service via smart mobile devices [1]. Smart mobile devices like smartphones, tablets and wearables are equipped with various built-in sensors, including GPS, camera, accelerometer, gyroscope and microphone among others; they have the potential for continuous environmental monitoring of air pollution, water quality, road condition for smart transportation, public safety and emergency preparedness [1], [2]. As the popularity and widespread use of these devices are continuously increasing, they appear to be the best candidates for being integrated to IoT-driven sensing applications. Performance of MCS platforms depends on the number of participants contributing to complete sensing tasks, making user recruitment a key challenge in MCS through proper incentivization [3], [4]. Proper recruitment policies allow the selection of users that are able to fulfill sensing tasks with high accuracy while minimizing system costs. On one hand, the central platform organizes and assigns tasks, thus sustaining a monetary cost to recruit and reward users for their contribution. On the other hand, users sustain costs for their contributions in terms of energy consumed for sensing and data subscription plan use for reporting. Several incentive strategies have been proposed in the literature with the aim of addressing the trade-off between platform and user utility [5].

Gamification is a common method to foster users collaboration [6] and it is a widely adopted technique nowadays [7]. Popular social platforms such as Foursquare, Twitter and Stack Overflow are well-known examples of platforms applying gamification in real environment. In gamified incentive methods, users receive badges as awards. These virtual rewards are meant to provide a sense of accomplishment in the users and to motivate them to participate actively and continuously [6]. As gamification is a psychological incentive method, the key to improve participation is user recognition and a thorough understanding of user behavior [8].

Trustworthiness of the submitted data is essential for applications like public safety, crisis management, and disaster preparedness [9]. In mission-critical applications, MCS platforms rely on user reputation as an indicator of data trustworthiness. Malicious users modify or alter data to deliberately provide disinformation. Upon detection of anomalies, such as outliers in the data set, the reputation of users providing such data reduces [10]. In the presence of malicious users, one of the main objectives of the crowdsensing platform is to determine the level of reliability/trustworthiness of each user. To achieve this objective, the platform stores information of user trustworthiness and reputation, which is dynamically updated on the basis of the quality of contributed data. It is worthwhile mentioning that not only malicious users can affect quality of data, but also inaccurate sensing reading, i.e., data coming from malfunctioning sensors [11].

In this paper, we propose a framework for trustworthiness-

978-1-5090-2482-7/16/$31.00 ©2016 IEEE

driven user recruitment in MCS platforms, consisting of three phases: i) user recruitment, ii) collaborative decision making, and ii) badge rewarding. The phases (ii) and (iii) define a game theoretic methodology used to incentivize participation, and incorporate gamification tools. Although few studies have provided preliminary analysis [12], [13], [14], the use of gamification in crowdsensing is still widely unexplored to this date. Application of a reward-based mechanism to rate users trustworthiness and stimulate user participation is the major contribution in our study. The collaborative decision making phase exploits a voting system derived from a repeated Subgame Perfect Equilibrium (SPE). Users voting truthfully obtain higher reward and ensure trustworthiness of the system by refusing to acknowledge low quality contributed data. Extensive simulation results show that our proposed framework improves platform utility by up to 50% and average user utility by 15% in comparison with previous research [15].

The paper is organized as follows. Section II presents background on related works and motivates the need for trustworthiness in user recruitment and incentives. Section III presents the trustworthiness-driven gamification model to recruit users in mobile crowdsensing systems. Section IV provides performance evaluation and analyzes the simulation results. Section V concludes the work and gives future directions.

II. Background and Motivation

With the integration of Mobile crowdsensing (MCS) into cloud computing, Internet of things and wearable technologies, MCS has enabled environmental monitoring, infrastructural management and social computing applications [16]. User recruitment is essential for the success of MCS. For such reason, policies to foster user participation have been largely investigated. Several comprehensive surveys review current methodologies to design incentive mechanisms in MCS systems [3], [5], [17].

Gamification employs game mechanisms in non-gaming contexts to motivate active user participation [6]. Gamification-based incentivization within the MCS context has received limited attention so far [18], [8], [19]. In crowdsourcing, use of gamification through badge awards is studied for a popular platform like Stack Overflow [7], and has been shown to improve motivation of users.

Xie et al. [20] propose an incentive mechanism composed of a rating system and a reward-based scheme. To allocate rewards between all users, a reputation protocol is employed to investigate users' history and eliminate users with poor reputation. However, new coming users are vulnerable to elimination as they have little chance of building a reputable history in a short time. We exert Subgame Perfect Equilibrium (SPE) in a game-theoretic voting phase. The output of this game is the reward granted on the basis of the utility of the data provided and the truthfulness of users' votes. The authors in [21] deduced a subgame perfect equilibrium as a bidding function to make payments more efficient to the users.

In this paper, we use both game theoretic monetary incentives and gamification methods unlike previous studies leveraging only monetary-based incentives [21], [22]. Because the evaluation of data reliability in MCS has received little attention so far, we propose a game-theoretic approach to model the interactions among users. In this game, a voting phase is formulated to evaluate the quality of the crowd-sensed data.

Table I
Notation used in the paper

Notation	Description
n	Number of participants in each
T_S	Set of tasks handled by the users in the set S
W_τ	Number of winners at t-th recruitment
$N_i(t)$	Number of assigned votes to user i at time t
w_j	Vote capacity of user-j
r_i	Submitted reading of user-i
Val_i	Task value of user-i
x_j^i	Actual vote of user-j for user-i
$R_i^{'}(t)$	Updated trustworthiness of user i at the end of $t_i + \delta$
λ_s	Dissimilarity threshold
γ_r	Rewarding threshold
$S_r^{ij}(t)$	Similarity indicator of task readings of users-i and j at time-t
ρ_m	Malicious user probability
$\int$	Probability of negative votes for a malicious user
Δ_{ij}	Difference between the values of sensing tasks of user-i and j
δ	Delay time between the 1st and 2nd phase
t_i	Submission time of task-i
$t_i + \delta$	Collaboration time
$\tau_{duration}$	Duration of t-th recruitment
V_i	Total vote capacity for user-i at the first phase
${p_i}^t$	Total Payment to user-i at t-th recruitment
v^R	Total values of the tasks in the platform
$R_i(t)$	Trustworthiness of user-i at the end of time-t
${c_i}^t$	Total sensing cost to user-i at t-th recruitment
"HI-award"	Category of users receiving a high reward
"LO-award"	Category of users receiving a low reward

III. System Model

The proposed framework is composed of the user recruitment, game theoretic collaborative decision making and gamification-based badge rewarding phases. The proposed model considers $n > 1$ users to perform submitted sensing tasks through built in sensors in mobile devices during each assignment process.

A. User Recruitment

The following methods are used to recruit users in the first phase: 1) Trustworthy Sensing for Crowd Management (TSCM) [10], which introduces statistical reputation-awareness to MSensing [23] and 2) SONATA [15]. Both schemes consist of two steps, namely the user selection and rewarding phases. The proposed approach here, adopts only the first stage of TSCM or SONATA based on its operation mode, i.e., statistical or vote-based. The two methods (i.e.,

TSCM and SONATA) differ in the way they ensure trustworthiness. TSCM is a *reputation-based policy*, i.e., instantaneous user reputation is statistically calculated based on true and false sensor readings. On the contrary, SONATA, being a pure *vote-based policy*, adopts Sybil detection techniques in online social networks [24] and determines the instantaneous user reputation on the basis of votes cast by other users sensing the same phenomenon.

MSensing is a user-centric reverse auction-based incentive mechanism. Users join the auction with their sensing costs (i.e., bids) as they are guaranteed that no user will be rewarded less than its bid in the auction [23]. The recruitment is completed in two steps, winner selection and reward determination. MSensing aims at maximum platform and user utility, and it addresses the truthfulness vulnerability introduced by the bidding mechanism. Truthfulness denotes the cases in which users aim to increase their incomes by bidding higher than the actual sensing costs. MSensing addresses this issue by selecting the winners based on their marginal contributions to the total value of the sensed tasks and their sensing costs, and sorts the users in descending order based on the marginal gain of the platform for recruiting each participant. User trustworthiness is computed by TSCM scheme based on the recent and past readings of corresponding participant.

SONATA ensures trustworthiness through user votes. The trustworthiness of user-i at time t is calculated as the summation of total votes normalized by overall vote capacity as follows:

$$R_i(t) = \frac{\sum_{j|c_{ij}=1} w_j x_j^i R_j(t)}{\sum_{j|c_{ij}=1} w_j R_j(t)}. \quad (1)$$

Equation (1) defines w_j as the vote capacity of user-i, x_j^i is the actual vote of user-i and R_j is the trustworthiness of user-j at time-t. In SONATA, the calculation of trustworthiness depends on the votes from the other users and the initial reputation. The vote-based user recruitment under proposed scheme in this paper, defines user reputation based on the quality of submitted data as opposed to SONATA where each user votes for a new user based on the similarity score of the sensed data. In SONATA, each user casts a negative vote for a malicious user with a certain probability, $\int$.

The proposed method in this paper makes the second phase adaptive such that the vote capacity of a user is increased only if the user provides *useful data*. Next section provides more details on the collaborative decision making mechanism.

Given n users are recruited by the time t_i, the platform needs to receive all captured data after a specific offset time δ by the end of $t_i + \delta$. At time $t_i + \delta$, user collected data is submitted to the platform, and all the participants are aware of task value.

B. Collaborative decision making

In collaborative decision making phase, all users interact in a game and make decisions sequentially based on the submitted value. We formulate the problem as a Sub-game Perfect Equilibrium (SPE). In SPE, players participate in a subset of a game, and their strategy represents a Nash Equilibrium [25]. In every sub game, each player behaves rationally and independently.

We define a successive sub-game describing the users' strategy. In this sub-game each task is assigned to m users. Each user has two available choices: participate in the voting phase or not to participate. The strategy each user adopts is defined by a tuple, $\{V, N\}$, where V denotes that the user is voting, and N signifies that user is not voting. During the voting phase, the user casting a vote is denoted as the *voter*, and the user receiving the vote is the *voted*. Users are not obliged to vote; thus they can decide either to remain idle (i.e., not voting) and obtain a payoff equal to zero or to participate in voting game and increase their income. Besides the user trustworthiness of each user that is assigned in the recruitment phase, participants have the chance of increasing their trustworthiness by providing feedback about the other users' sensed value. The vote capacity $V_i^{'}(t)$ augments while the users vote to define trustworthiness of data produced by the other contributors. Augmenting the vote capacity is an incentive to motivate the users in taking part in the voting game. Eventually when a user decides to vote, the algorithm compares data similarity of both voter and voted. If the dissimilarity score of the values is below a certain threshold λ_s, the vote capacity of both users increases. Otherwise, the vote capacity of the voted decreases.

The last step of the game is to determine vote reliability. One of the main objectives of this study is to guarantee that truthful users receive higher ratings with respect to dishonest ones. For this, the latter type of users lose credit upon casting untruthful votes. As a result, when the vote capacity is increased/decreased it has a direct impact on their reputation as per (1) and, in turns, on the achieved reward.

The collaborative voting phase consists of two steps. The first step assesses the quality of the contributed data. For quality assessment, the users compare the data to be judged with the data they own at time $t_i + \delta$. This procedure is performed sequentially. When the dissimilarity of data held by voter and voted is above a threshold λ_s, the voter casts a negative vote. In the case of a negative vote, the platform decreases the trustworthiness of the crowdsensed data. Consequently, the voting capacity of the voter, if casting truthful negative votes, increases. On the contrary, when a voter casts untruthful votes, the platform decreases its voting capacity.

The second step investigates the accuracy of the assigned votes. As the platform has knowledge on the value of the tasks, it can judge whether the voters have provided genuine votes or not. As the final step, the platform diminishes the vote capacity of users that cast misleading votes. By applying this game between the users, the objective is to incentivize users to collaborate for qualifying the value of sensed tasks. When users cast correct votes, they increase their own voting capacity. Thus, a malicious user who intends to forge the platform and votes negatively for a user who provided trustworthy data, the platform reduces its reputation accordingly. As a consequence users are encouraged to provide genuine feedback about the

value of data captured by the other recruited users.

Practically, the platform rates the participants on the basis of the following criteria: i) the value of the data they contribute, ii) their voting trustworthiness. The rating scale is assigned according to $\Delta_{ij}(t) = |r_i - r_j|$, which is the difference between the readings of user i and j. The calculated binary similarity indicator is used in the following section for badge rewarding. The binary similarity indicator between user-i and user-j at time-t, $S_r^{ij}(t)$ indicates whether the data similarity criterion is satisfied or not and is defined as follows:

$$\Delta_{ij}(t) = |r_i - r_j| \tag{2}$$

$$S_r^{ij}(t) = \begin{cases} 1 & \text{if } \frac{\Delta_{ij}(t)}{\max\{r_i\}} \leq \lambda_s; \\ -1 & \text{if } \frac{\Delta_{ij}(t)}{\max\{r_i\}} > \lambda_s. \end{cases} \tag{3}$$

At the end of the collaborative voting phase each user earns a total voting capacity, which is computed by taking into account positive and negative votes cast during each time slot. The vote capacity of user i at time t+δ is calculated as follows:

$$V_i^{'}(t) = \frac{\sum_{j=1|j\in N_i(t)}^{|N_i(t)|} S_r^{ij}(t)}{N_i(t)}, \tag{4}$$

where $S_r^{ij}(t)$ is the similarity rating feedback that user i receives from its neighbors. At the end of the voting phase, reputation $R_i^{'}(t)$ of each user is re-calculated by using two parameters, namely the new collaborative vote capacity (5), and the user's reputation $R_i(t)$ which is defined during recruitment phase (1).

$$R_i^{'}(t) = V_i^{'}(t) + R_i(t). \tag{5}$$

To achieve higher vote capacity, users are motivated to provide correct feedback. The updated reputation is utilized in the next step as the criteria for reward assignment. As a consequence, users never earn rewards upon providing hostile and misleading feedback to the system.

C. Badge Rewarding

Typically incentive mechanisms focus on single actions, while gamification considers their overall contribution [26]. Therefore, applying gamification to long term applications is beneficial. We consider a reward-based gamification method, where the users receive badges from the platform. In the reward-based approach, the platform awards badges when users satisfy a certain reward level entry [7]. Distinguishing reliable users increases both platform and user utility. Indeed, this corresponds to having the crowdsourcer recruiting users that contribute qualified data in a trustworthiness fashion.

Easley et al. [7] propose two reward allocation mechanisms: i) absolute standard mechanism M_α, and ii) a relative standard mechanism M_ρ. The absolute standard mechanism issues badges when users provide a certain level of effort. The relative standard mechanism awards badges when users provide certain level of effort in comparison with the top contributor. The relative policy is more robust than the absolute one, as it works regardless of particular conditions of the platform such as the number of participants.

In this paper, we adapt relative standard mechanism to select the winners of awards; when users' vote capacity reaches a certain level, the platform awards them with a badge. In this phase, the users are grouped into two categories. The users receiving a high reward are grouped in the "HI-award" class, while the users receiving a low reward are associated to the "LO-award" class. (The platform distinguishes the user's category according to their collaboratively computed voted capacity, which is determined in (5).

$$R_i(t) = \begin{cases} R_i^{'}(t) & \text{if } V_i > \gamma_r, \quad \text{"HI-award"}; \\ R_i(t) & \text{if } V_i < \gamma_r, \quad \text{"LO-award"}. \end{cases} \tag{6}$$

When users provides reliable data to the platform, they build their new reputation according to $R_i^{'}(t)$ (see (6)). Consequently, the chance of achieving high award increases.

IV. Performance Evaluation

We simulate the proposed mechanism and compare the system performance of SPE-based user recruitment with the benchmark mechanism SONATA. The SPE-based user recruitment operates in two modes, namely the vote-based (*vote-based reputation + SPE*) and statistical reputation-based (*statistical reputation + SPE*) modes. The former adopts the user selection mechanism of SONATA [15] whereas the latter adopts the user selection phase of TSCM [10], which is a statistical reputation-based method.

A. Simulation Settings and Performance Evaluation Metrics

Similar to [15], the simulation environment consists of a 1000×1000 terrain with 1000 users, and a user is interested in a sensing task if the task is within 30 units of their range. We assume three different malicious user probabilities in the monitored terrain, 3%, 5% and 7%. The initial reputation of users is set to 70%, and varies during the crowdsensing event. The duration of an event is set to 30 minutes, and the platform assigns sensing tasks under various arrival rates, i.e. 20, 40, 60, 80, 100 tasks/min. When SONATA is used in the first phase for user recruitment, the probability of detecting a malicious user is assume to be 20%. If the dissimilarity score between two sensor readings is higher than 20%, the two readings are considered as two different readings/reporting of the same task. The value of a task is an integer that is randomly selected out of the interval [1, 5] whereas the bids/sensing costs take integer values from the interval [1,10]. Three metrics assess the performance of the proposed framework:

1) *Platform utility*: it measures the total received useful value from the participants deducted by the total payments awarded to the users.

$$U_{platform} = \sum_{\tau} \left(v^R(W_\tau) - \sum_i {p_i}^\tau \right), \tag{7}$$

where v^R is the total reputable values of the tasks in the platform. Note that in both (7) and (8) ${p_i}^\tau$ is the total

payment to the user-i whereas ${c_i}^\tau$ is sensing cost of user-i during t. The parameter W_τ represents the number of winners during the auction period $\tau_{duration}$.

2) *Average user utility*: It measures the difference between the payment received from the platform and the sensing cost. User utility is averaged by the total numbers of selected users in crowdsensing:

$$U_{user} = \frac{\sum_t((\sum_i {p_i}^\tau - \sum_i {c_i}^\tau)/|W_\tau|)}{\tau_{duration}}. \quad (8)$$

3) *Total amount of payment to malicious users*: it measures the reward given to malicious users.

B. Simulation Results

The first figure illustrates the effect of having three different malicious user percentages on the platform utility. As seen in Fig. 1, increasing the probability of having malicious users leads to better results in SPE-based user recruitment modes in comparison to the platform utility under SONATA. The reason is two-fold: 1) both SPE-based modes detect more malicious users, and, consequently, the payments to such users decrease leading to an increase in platform utility, 2) by incentivizing users to provide useful data, the values of received data outperform SONATA results. Fig. 1 shows that, by having $5-7\%$ malicious user percentage, the maximum improvement in platform utility is as high as 55% in reputation-based SPE mechanism. By setting the malicious population to 3% of total crowd population, an improvement in platform utility can still be expected but not as high as the other two scenarios. Indeed, this improvement is in average up to 13%.

Fig. 2 compares the three schemes in terms of the average user utility. As expected, the degradation of user utility is not significant. The main reason lies in the fact that the platform pays more to the users with high number of badges. Note that the statistical reputation-based method improves SONATA by on average 15% and outperforms the vote-based scheme. Indeed, in the vote-based scheme, the users during first voting phase use more vote capacity than in the statistical reputation-based scheme. As a result, their sensing cost augments, diminishing the utility. Having defined the metric in function of both cost and income, to maximize user utility with fixed incomes it is necessary to reduce the sensing cost.

Fig. 3 illustrates the total payment rewarded to malicious users under different task arrival times. SPE-based user recruitment provides significant improvements when compared to the baseline solutions like SONATA. The latter method rewards considerably malicious users while SPE-based techniques detect such users and do not reward them at all. Clearly in SONATA, the malicious users providing fake data and aim at misleading the recruiter platform by building bogus reputation and consequently reducing the system trustworthiness. More in detail, they manipulate their sensing value to satisfy a predefined upper threshold so that the platform recognizes them as trustworthy users. Nevertheless the platform continues to pay them until their reputation decreases reaching a lower threshold. At this point an adversary is identified, and the platform does not reward these users anymore. In the proposed framework, SPE-based techniques intently use badges to verify trustworthy users and identify them. Finally the platform pays only to trusted users to improve user and platform utilities.

V. Conclusion

We designed a gamification incentive framework to foster users participation in crowdsensing and to ensure trustworthiness. The framework adopts the winner selection mechanism from a previously proposed method, namely, Social Network-Aided Trustworthiness Assurance (SONATA) [15], and improves the rewarding step by integrating reputation of the users with the awarded badges. To achieve badges, users collaborate to build their reputation through a voting system, derived from a repeated Subgame Perfect Equilibrium (SPE). Extensive simulations prove that SPE method is trustworthy, and profitable for users and crowdsensing platforms. Moreover, based on simulation results, the proposed SPE method completely prevents the platform from paying to malicious users.

Acknowledgment

This material is based upon work supported by the U.S. National Science Foundation (NSF) under Grant Nos. CNS1464273 and CNS-1239423, and the funding from National Research Fund, Luxembourg in the framework of ECO-CLOUD and iShOP projects.

References

[1] R. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32–39, November 2011.

[2] W. Khan, Y. Xiang, M. Aalsalem, and Q. Arshad, "Mobile phone sensing systems: A survey," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 402–427, First 2013.

[3] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, and X. Mao, "Incentives for mobile crowd sensing: A survey," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, 2015.

[4] 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.

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

[6] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: defining gamification," in *Proceedings of the 15th Intl. academic MindTrek Conf.* ACM, 2011, pp. 9–15.

[7] D. Easley and A. Ghosh, "Incentives, gamification, and game theory: an economic approach to badge design," in *14th ACM Conf. on Electronic Commerce*, 2013, pp. 359–376.

[8] Y. Ueyama, M. Tamai, Y. Arakawa, and K. Yasumoto, "Gamification-based incentive mechanism for participatory sensing," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on*. IEEE, 2014, pp. 98–103.

[9] 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, Mar 2016.

[10] B. Kantarci and H. T. Mouftah, "Trustworthy sensing for public safety in cloud-centric internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 360–368, Aug 2014.

[11] T. Giannetsos, S. Gisdakis, and P. Papadimitratos, "Trustworthy people-centric sensing: Privacy, security and user incentives road-map," in *13th Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*, 2014, pp. 39–46.

[12] M. Talasila, R. Curtmola, and C. Borcea, "Crowdsensing in the wild with aliens and micropayments," *IEEE Pervasive Computing*, vol. 15, no. 1, pp. 68–77, Jan 2016.

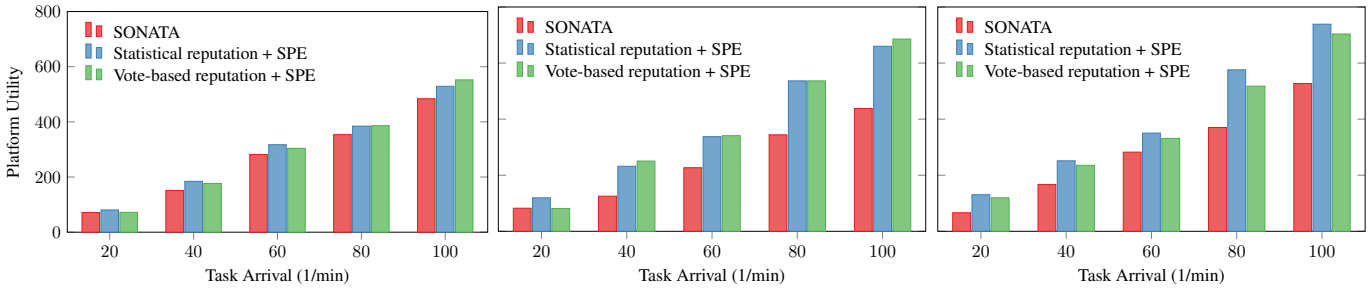

Figure 1. Platform utility vs. sensing task arrival rate for malicious user ratios of a) 3%, b) 5%, and c) 7%.

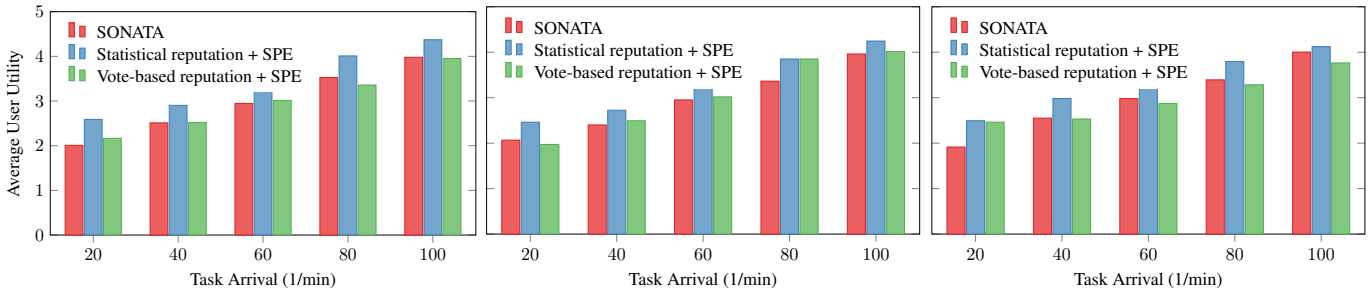

Figure 2. Average user utility vs. sensing task arrival rate for malicious user ratios of a) 3%, b) 5%, and c) 7%.

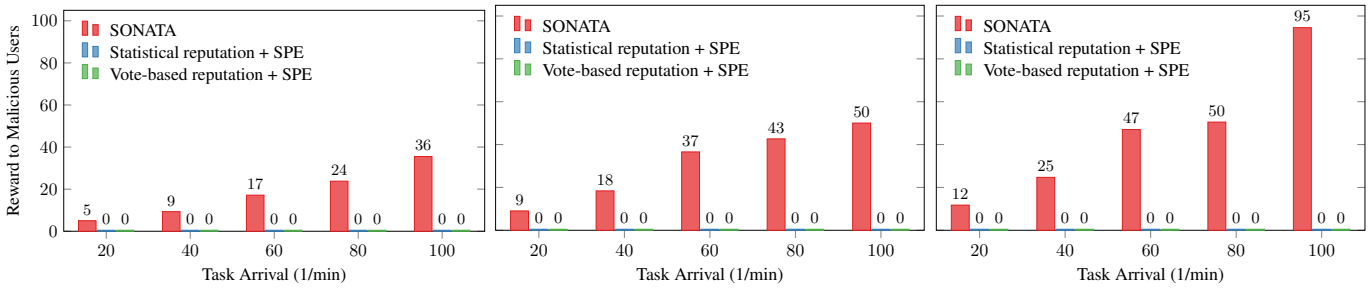

Figure 3. Reward to malicious users vs. sensing task arrival rate for malicious user ratios of a) 3%, b) 5%, and c) 7%.

[13] K. Han, E. A. Graham, D. Vassallo, and D. Estrin, "Enhancing motivation in a mobile participatory sensing project through gaming," in *IEEE Third Intl. Conf. on Privacy, Security, Risk and Trust and IEEE Third Intl. Conf. on Social Computing*, 2011, pp. 1443–1448.

[14] N. D. Lane, M. Mohammod, M. Lin, X. Yang, H. Lu, S. Ali, A. Doryab, E. Berke, T. Choudhury, and A. Campbell, "Bewell: A smartphone application to monitor, model and promote wellbeing," in *5th ICST Conf. on pervasive computing technologies for healthcare*, 2011, pp. 23–26.

[15] B. Kantarci, K. G. Carr, and C. D. Pearsall, "Sonata: Social network assisted trustworthiness assurance in smart city crowdsensing," *Intl. J. of Distributed Systems and Technologies*, vol. 7/1, pp. 59–78, 2016.

[16] Y. Xiao, P. Simoens, P. Pillai, K. Ha, and M. Satyanarayanan, "Lowering the barriers to large-scale mobile crowdsensing," in *Proc. 14th Workshop on Mobile Computing Systems and Applications*, 2013, p. 9.

[17] Y. Liu and C. Miao, "A survey of incentives and mechanism design for human computation systems," *arXiv preprint arXiv:1602.03277*, 2016.

[18] F.-J. Wu and T. Luo, "WiFiScout: A crowdsensing WiFi advisory system with gamification-based incentive," in *IEEE 11th Intl. Conf. on Mobile Ad Hoc and Sensor Systems (MASS)*, 2014, pp. 533–534.

[19] R. Kawajiri, M. Shimosaka, and H. Kashima, "Steered crowdsensing: incentive design towards quality-oriented place-centric crowdsensing," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 2014, pp. 691–701.

[20] H. Xie, J. Lui, J. W. Jiang, and W. Chen, "Incentive mechanism and protocol design for crowdsourcing systems," in *52nd Allerton Conf. on Communication, Control, and Computing*. IEEE, 2014, pp. 140–147.

[21] J. Sun, "Behavior-based online incentive mechanism for crowd sensing with budget constraints," *arXiv preprint arXiv:1310.5485*, 2013.

[22] L. G. Jaimes, I. Vergara-Laurens, and A. Chakeri, "Spread, a crowd sensing incentive mechanism to acquire better representative samples," in *IEEE Intl. Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. IEEE, 2014, pp. 92–97.

[23] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing," in *Proc. of the 18th Annual Intl. Conf. on Mobile computing and networking*. ACM, 2012, pp. 173–184.

[24] Z. Yang, J. Xue, X. Yang, X. Wang, and Y. Dai, "VoteTrust: Leveraging Friend Invitation Graph to Defend against Social Network Sybils," *IEEE Trans. on Dependable and Secure Computing*, vol. 13/4, pp. 488–501, July 2016.

[25] J. Moore and R. Repullo, "Subgame perfect implementation," *Econometrica: Journal of the Econometric Society*, pp. 1191–1220, 1988.

[26] A. Ghosh, "Game theory and incentives in human computation systems," in *Handbook of Human Computation*. Springer, 2013, pp. 725–742.