DTRF: A Dynamic-Trust-based Recruitment Framework for Mobile Crowd Sensing System

Yali Gao, Xiaoyong Li, Jirui Li, Yunquan Gao
Key Laboratory of Trustworthy Distributed Computing and Service (BUPT) Ministry of Education
Beijing University of Posts and Telecommunications
Beijing, P.R.China
Email: {gaoyalibupt, lxyxjtu, ljrokyes}@163.com, gaoyunquan@bupt.edu.cn

***Abstract*—Mobile Crowd Sensing (MCS) is a promising paradigm in which mobile users collect and share sensor data from their local environment using wireless mobile devices. The inherent openness of this platform and the selfishness of individuals make it easy to contribute low-quality sensor data, so the recruitment of suitable participants who are trustable and contribute high-quality sensor data, becomes a fundamental requirement for MCS system. In this paper, we propose a dynamic-trust-based recruitment framework (DTRF) for MCS system. Real-time direct trust and lightweight feedback aggregation trust are combined to select the well-suited participants. In addition, we adopt an adaptive weight allocation approach to calculate the overall trust degree of the participants. Theoretical analysis and extensive simulation confirm that DTRF can efficiently select the trustworthy participants and effectively stimulate the participants to contribute high-quality sensor data and thus get high task completion rate and data quality.**

***Index Terms*—recruitment framework; mobile crowd sensing system; participatory sensing; trust**

I. Introduction

With the widespread prevalence of sensor-embedded mobile computing devices, the combination of mobile computing, crowdsourcing computing, participatory sensing [1], wireless sensor network, and online social network brings about a novel sensing paradigm of Internet of Things (IoT), known as Mobile Crowd Sensing (MCS) [2], [3]. In MCS system, participants with sensor-enhanced mobile devices are able to contribute and share data from the physical world, enabling a broad range of applications.

The inherent openness of mobile crowd sensing system makes the trustworthiness of the sensor data is a big concern for the application server. The recruitment framework recruits enough stable and optimal groups of participants to ensure the accuracy, coverage, and timeliness of the sensing results. The dynamic-trust-based recruitment framework makes sure of the security, trustworthiness and dependability of the MCS system.

The biggest challenge of recruitment framework for MCS system is the selection of trustworthy participants. Although the existing achievements [4], [5] have greatly promoted the development of correlational research. A lightweight and dependable recruitment framework designed specifically for MCS system is still lacking.

Inspired by the idea of an expanded trust evaluation approach in [6], in DTRF, we define trust as a quantified belief by the MCS platform with respect to the the data quality of the mobile device within several recent time windows. This definition belongs to an approach based on trusted third party (TTP). The MCS platform acts as the TTP, where many mobile devices should be registered to be a member of the MCS system. The key features of DTRF go beyond those of existing schemes in terms of the following aspects. Firstly, the feedback trust calculation is lightweight. Secondly, an Adaptive Weighting Method is proposed to calculate the overall trust degree of the participants. This method can overcome the subjectivity of traditional weighting methods for trusted attributes, improve the fairness and rationality of the trust evaluation process, and motives the participants to submit high-quality sensor data.

This paper will provide both theoretical analysis and simulation results to validate the designs of the DTRF. The rest of this paper is organized as follows. Section II gives an overview of related work. The DTRF's architecture and details are described in Section III. Section IV provides the details of trust calculation mechanism. The simulation setup and results are presented in Section V. Finally, Section VI concludes this work and suggests some future directions.

II. Related Work

Research on recruitment framework for MCS received considerable attention from scholars. A number of studies have proposed mechanisms for MCS [4], [7]–[11] However, these mechanisms suffer from various limitations such as the inflexibility of even the lacking of the trust evaluation scheme. As such, we mainly considered the trust mechanism in participant recruitment, which is lightweight and dependable.

Amintoosi *et al.* [4], [7] proposed an application-agnostic reputation framework for social participatory sensing systems. Five factors are considered to calculate the trust of participants. However, the weight allocation of trust factors depends on the nature of the task, which has subjective and manual factors to some extent and lacks of self-adaptability.

Yang *et al.* [8] proposed a reputation management model to classify the gathered data for participatory sensing. To help classify participants as trustworthy or not, the model considers three factors of trustworthiness, but the factors are weighted

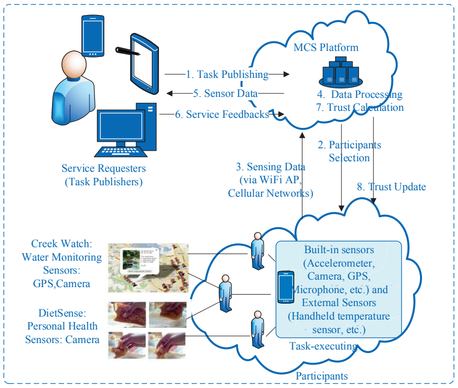


Fig. 1. A Reference Framework for MCS System.

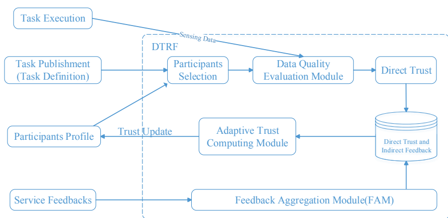


Fig. 2. Recruitment Framework's Steps, Inputs, and Outputs

by analysts and organizers, which is manually and subjectively to some extent and lacks the adaptability.

Reddy *et al.* [9] proposed a recruitment framework for participatory sensing systems which aims at identifying well-suited participants for data collection. Temporal and geographic availability as well as participation reputation are considered in the qualifier component. The assessment component selects a subset of participants to do the sensing task, who maximize coverage over task specific area. Li *et al.* [12] proposed a dynamic participant recruitment of Mobile Crowd Sensing for heterogeneous sensing tasks, which mainly considered the heterogeneity of tasks.

III. DTRF's Architecture and Details

In this section, we first present the architecture of the proposed recruitment framework in MCS system. Then we will focus on the details of feedback aggregation module.

A. The Architecture of DTRF

In the DTRF mechanism, sensing task is characterized by a tuple $T{=}\langle e,d,l,p,T_{th}\rangle$, where e is the earliest time to execute the task, d is the deadline of the data submission, l is the location of the sensing task, p is the expected number of participants to execute the task and T_{th} is the task's minimum requirement on trust degree.

The architecture of the DTRF mechanism is illustrated in Fig. 1. Firstly, service requesters as the role of task publishers, publish the sensing task attached a tuple $T{=}\langle b,e,l,p,T_{th}\rangle$ on the MCS platform (Step 1). The participant, whose location is in the range of the task and trust degree is not lower than the task's threshold T_{th}, can be selected to the candidate list and accept the task (Step 2). The first p accept the task will have the priority to execute it and upload the collected sensor data to the platform using existing communication infrastructure such as WiFi access point or cellular networks (Step 3). The platform will process and evaluate the uploaded data to provide the sensing service, and a real number between 0 and 1, which denotes the quality of the sensor data, will be stored in the trust database (Step 4). The service requesters will give service feedbacks to the platform when they receive the sensing services (Step 5 and 6). Finally, the platform will process the feedbacks of the service requesters, give rewards or penalties to the relevant participants, and update their OTD values (Step 7 and 8).

B. Feedback Aggregation Module

Feedback can provide great references in evaluating the trustworthiness of the MCS entities. Considering the large-scale MCS computing environment which schedules thousands of mobile devices and processes millions of requests per second, the delay caused by trust system can be a big problem. We adopt a lightweight feedback aggregation mechanism, which can not only improve the efficiency of the trust system greatly but also reduce the system risk effectively.

IV. Trust Calculation Model

In view of the fact that the higher the participant's overall trust degree, the higher his/her data quality will be. In this section, we will elaborate the proposed trust calculation model.

A. The Definition of Trust

Let $X=\{x_1,x_2,\ldots,x_N\}$ denote the entity set of the MCS system, where each $x_k(k=1,2,\ldots,N)$denotes an entity, and N is the number of entities. There are two roles in the trust model: service requesters and task executors.

We use the term "Trust" to represent the quantified belief in the correctness and reliability of one service requester on one task executor. The trust degree of service requester x_i on task executor x_j changes over time. Each behavior of x_j will cause x_i' trust reevaluation on him/her. This dynamic characteristics of the trust relationship should be reflected by the trust model.

B. Real-Time Direct Trust Computation

Direct trust is the trust of x_i on x_j based on the direct contact behaviors in the recent past. We regard the data quality as the degree of service requester's satisfaction. Let $(e_{ij}^{(1)},e_{ij}^{(2)},\ldots,e_{ij}^{(h)})$ denote the satisfaction sequence in recent h direct contacts, where $e_{ij}^{(k)}(0\leqslant k\leqslant h\leqslant H, 0\leqslant e_{ij}^{(k)}\leqslant 1)$ denotes the satisfaction degree of service requester x_i on task executor x_j in the recent k_{th} direct contacts and $e_{ij}^{(1)}$,$e_{ij}^{(h)}$ denote the earliest and latest effective record respectively. H is the maximum number of effective history records. Thus, we define the direct trust degree of x_i on x_j as:

$$T_1(x_i,x_j)=\begin{cases}\sum_{k=1}^{h} e_{ij}^{(k)}\frac{\gamma(k)}{\sum_{k=1}^{h}\gamma(k)}, & h\neq 0\\ 0, & h=0\end{cases}\qquad(1)$$

where $\gamma(k)\in[0,1]$ denotes the weight of direct trust record at different moments. In the light of people's cognitive custom on

Algorithm: Task Assignment

```
Input: Service requester x_i publishes a task
       T =< e, d, l, p, T_th >, set S
Output: P
P ← ∅, S' ← ∅;
for (x_j ∈ S) do
  if (Γ(x_i, x_j) ⩾ T_th && x_j is in location l) then
    S' = S' + {x_j}
  end if
end for
while the size of P is smaller than p do
  if (x_j ∈ S' && x_j accept the task) then
    P = P + {x_j};
    Assign the sensing task to x_j;
    x_j executes the sensing task assigned to him/her;
  end if
end while
```

TABLE I
THE PARAMETERS AND THEIR POSSIBLE VALUES

Symbol	Description	Possible Values
N	number of the participants	200
T	Number of the tasks	5
H	Maximum number of effective records	10
λ	The ratio of P3 in all mobile nodes	0.1,0.4,0.8
o	Number of locations (towers)	20
m	Number of tasks	60,70,80,90,100
n	Number of candidate participants	100,200,300,400,500
γ	Coverage threshold	0.3,0.4,0.5,0.6,0.7

trust, the latest interaction record should be given more weight than the previous records. Thus, we define the attenuation function as:

$$\gamma(k) = \lambda^{h-k}, (k = 1, 2, \ldots, h) \tag{2}$$

where the exponential term λ^{h-k} $(0 < \lambda < 1)$ reduces the impact of the history data, which achieves ageing.

Compared with other trust models for MCS system, the calculation of direct trust degree in DTRF, which combines attenuation function with timestamps, has the following advantages: Firstly, it improves the accuracy of trust quantification from the perspective of representativeness and objectiveness. Secondly, introducing the maximum number of effective history records can help remove the previous data and relieve the pressure of data storage.

C. Lightweight Feedback Trust Computation

Feedbacks aggregation module collects service feedbacks generated by the service requesters, and aggregates these feedbacks to yield the indirect feedback trust. After a service requester receives sensor data, the service requester will provide his/her feedbacks for other service requesters as a reference in future interactions.

Inspired by Whitby's Beta feedback system [13], we use the Beta probability density functions to compute feedback trust degree:

$$T_2(x_i, x_j) = \frac{p_j + 1}{p_j + n_j + 2} \tag{3}$$

where p_j is the number of positive evaluations ($\geqslant 0.5$) that task executor x_j received from all service requesters whom he/she has served for, and n_j is the number of negative evaluations (< 0.5) that x_j received.

In Equation (3), as expected, the feedback trust degree of a new joined task executor is 0.5, where $p_j = n_j = 0$. This idea is based on the research result in [14], whose authors pointed out that the suspicion of new participants is socially inefficient since only a limited number of participants are malicious in the MCS system. This approach can give a chance for new participants to enter the MCS system until they are proved untrustworthy.

It is easily to find that our feedback trust computation approach is lightweight, which only involves simple counting operation and arithmetic operations.

D. Adaptive OTD Aggregation

There are two trust evaluation factors, expressed as $T_1(x_i, x_j)$, $T_2(x_i, x_j)$. w_1 and w_2 are the weights assigned to $T_1(x_i, x_j)$ and $T_2(x_i, x_j)$ respectively. Thus, we define the overall trust degree (OTD) $\Gamma(x_i, x_j)$ as:

$$\Gamma(x_i, x_j) = w_1 \times T_1(x_i, x_j) + w_2 \times T_2(x_i, x_j) \tag{4}$$

where the sum of w_1 and w_2 is equal to 1.

$$w_1 = \frac{T_1(x_i, x_j)}{T_1(x_i, x_j) + T_2(x_i, x_j)} \tag{5}$$

$$w_2 = \frac{T_2(x_i, x_j)}{T_1(x_i, x_j) + T_2(x_i, x_j)} \tag{6}$$

Obviously, in Equation (5) and (6), the greater the value of trust evaluation factor, the greater the weight. That is, give more weight on the more trustworthy evaluation factor, which is in line with the cognitive pattern of human beings on trust.

E. Algorithm Realization

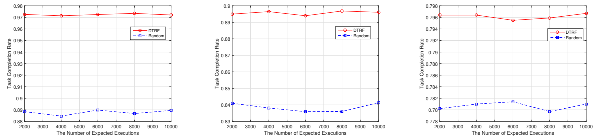
S: Online participants.
S': Online participants who meet the task's requirements.
P: The task executors set.

V. EXPERIMENTS AND EVALUATION

In this section, we first describe how to set up the simulation experiments in Section V-A. Then, the simulation results are described in Section V-B.

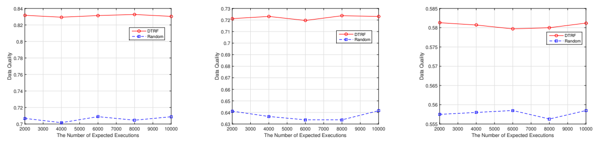
A. Simulation Setup

To measure the performance and accuracy of the proposed DTRF, we implemented a simple simulator based on NetLogo [15]. NetLogo is a very popular multi-agent programmable modeling tool based on Java in the AI community, and can easily simulate interactions among the independent and parallel service requesters and task executors. Simulation parameters and their possible values used in the experiments are described in Table I. In our simulation tests, there are three kinds of task executors with different behavior patterns: benign nodes (marked as P1, who are more likely to submit high quality sensor data), malicious nodes (marked as P2, who submit low quality sensor data or don't submit the sensor data on time), sometimes benign and sometimes malicious



(a) $\lambda = 0.1$ (b) $\lambda = 0.4$ (c) $\lambda = 0.8$

Fig. 3. Task Completion Rate with Varying λ



(a) $\lambda = 0.1$ (b) $\lambda = 0.4$ (c) $\lambda = 0.8$

Fig. 4. Data Quality with Varying λ

nodes (marked as P3, who may launch on-off attacks by submitting high-quality sensor data in order to improve the OTD value and submitting low-quality sensor data randomly or at a specific time). In this paper, we assume that the roles of task publishers and task executors are fixed and can not be changed. We make the simulation in different network environment, where the value of λ is 0.1, 0.4, 0.8 respectively.

Due to the fact that we focus on the centralized authority based trust evaluation mechanism in MCS, not the dynamic and heterogeneous nature of the sensing tasks, there is little significance to compare our model with existing models which have different assumptions. Thus, we compare the proposed DTRF with the random model.

B. Simulation Results

We compare the proposed DTRF with the random model from the perspective of task completion rate of all sensing tasks and the average data quality of all sensing tasks. The result for the task completion rate with varying λ is shown in Fig. 3. As we can see that the curve of our model almost maintains stable as the number of task's expected executions increases, while the curve of Random model fluctuate much more, which means our mechanism has the advantage of fine stability regardless of how busy the system is. It is clear that as the ratio of P3 in all mobile nodes increases, the task completion rate is still higher than that of the Random model, which means our mechanism has the advantage of dynamic adaptability in highly dynamic environment.

Again, for the same settings, we test the data quality and our result is shown in Fig. 4. The curves follow the similar trend as Fig. 3, which is the expected result. The reason is the overall trust degree of the participants affects both the task completion rate and data quality, and vice versa. From Fig. 3 and Fig. 4, we can see that our recruitment framework can achieve better performance in terms of selecting trustworthy participants and improving task completion rate than the Random model in different kinds of network environments.

VI. Conclusions and Future Work

This paper proposed a dynamic-trust-based recruitment framework for the mobile crowd sensing system. The theoretical analysis and simulation results confirmed that the proposed recruitment framework can achieve good performance in terms of selecting trustable participants and improving task completion rate and data quality. As for future work, we intend to consider about other factors that influence the trust degree of the participants, such as the availability of participants in terms of temporal and geographic coverage of the sensing area. Furthermore, we will consider the recruitment framework with cost constraint.

Acknowledgment

This work was supported by the National Nature Science Foundation of China (No. 61370069, 61672111), Fok Ying Tung Education Foundation (No. 132032), Beijing Natural Science Foundation (No. 4162043), and the Cosponsored Project of Beijing Committee of Education.

References

[1] B. Guo, Z. Yu, X. Zhou, and D. Zhang, "From participatory sensing to mobile crowd sensing," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on*, pp. 593–598, March 2014.

[2] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Communications Magazine*, vol. 49, pp. 32–39, November 2011.

[3] H. Ma, D. Zhao, and P. Yuan, "Opportunities in mobile crowd sensing," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 29–35, 2014.

[4] H. Amintoosi and S. S. Kanhere, "A reputation framework for social participatory sensing systems," *Mobile Networks and Applications*, vol. 19, no. 1, pp. 88–100, 2014.

[5] H. Amintoosi and S. S. Kanhere, "A trust-based recruitment framework for multi-hop social participatory sensing," in *2013 IEEE International Conference on Distributed Computing in Sensor Systems*, pp. 266–273, May 2013.

[6] L. J. Hoffman, K. Lawson-Jenkins, and J. Blum, "Trust beyond security: An expanded trust model," *Commun. ACM*, vol. 49, pp. 94–101, July 2006.

[7] H. Amintoosi and S. S. Kanhere, "Providing Trustworthy Contributions via a Reputation Framework in Social Participatory Sensing Systems," *ArXiv e-prints*, Nov. 2013.

[8] E. Shakshuki, M. Younas, H. Yang, J. Zhang, and P. Roe, "Using reputation management in participatory sensing for data classification," *Procedia Computer Science*, vol. 5, pp. 190 – 197, 2011.

[9] S. Reddy, D. Estrin, and M. Srivastava, *Recruitment Framework for Participatory Sensing Data Collections*, pp. 138–155. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[10] W. Nan, B. Guo, S. Huangfu, Z. Yu, H. Chen, and X. Zhou, "A cross-space, multi-interaction-based dynamic incentive mechanism for mobile crowd sensing," in *Ubiquitous Intelligence and Computing, 2014 IEEE 11th Intl Conf on and IEEE 11th Intl Conf on and Autonomic and Trusted Computing, and IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UTC-ATC-ScalCom)*, pp. 179–186, Dec 2014.

[11] K. L. Huang, S. S. Kanhere, and W. Hu, "On the need for a reputation system in mobile phone based sensing," *Ad Hoc Netw.*, vol. 12, pp. 130–149, Jan. 2014.

[12] H. Li, T. Li, and Y. Wang, "Dynamic participant recruitment of mobile crowd sensing for heterogeneous sensing tasks," in *Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on*, pp. 136–144, Oct 2015.

[13] A. Whitby, A. Jsang, and J. Indulska, "Filtering out unfair ratings in bayesian reputation systems," in *Proceedings of the Seventh International Workshop on Trust in Agent Societies*, pp. 106–117, 2004.

[14] E. J. Friedman* and P. Resnick, "The Social Cost of Cheap Pseudonyms," *Journal of Economics & Management Strategy*, vol. 10, pp. 173–199, 06 2001.

[15] "NetLogo." http://ccl.northwestern.edu/. Accessed August 1, 2016.