Trust-based IoT Cloud Participatory Sensing of Air Quality

Jia Guo[a], Ing-Ray Chen[a,1], Ding-Chao Wang[b], Jeffrey J.P. Tsai[c], Hamid Al-Hamadi[d]

[a] *Department of Computer Science, Virginia Tech, USA, {jiaguo, irchen}@vt.edu*

[b] *Department of Information Management, Southern Taiwan University of Science and Technology, Taiwan, wangdc.stut@gmail.com*

[c] *Department of Bioinformatics and Biomedical Engineering, Asia University, Taiwan, jjptsai@gmail.com*

[d] *Department of Computer Science, Kuwait University, Kuwait, hamid@cs.ku.edu.kw*

Abstract - In this paper we present a case study of IoT cloud participatory sensing where a user sends a query to the cloud to the air quality of a location at a particular time to decide if it should enter the location based on its susceptibility to the air quality detected. All IoT devices (e.g., smart phones carried by humans or smart cars driven by humans) capable of detecting air quality can act as participants and submit sensing reports to the cloud for sensing result aggregation. The major challenge is the selection of trustworthy participants because not all IoT devices will be trustworthy. We leverage a "Trust as a Service" (TaaS) cloud utility to address the issue of selecting trustworthy participants. Using real traces of ozone (O3) levels and mobility traces of users in the O3 community of interest (O3COI) group in the city of Houston, we demonstrate that TaaS outperforms contemporary IoT trust protocols in selecting trustworthy participants. We compare the performance of the TaaS cloud utility with two contemporary IoT

[1] Corresponding Author.

trust protocols for supporting trust-based IoT participatory sensing applications. With the help of the TaaS cloud utility, a user in this O3COI group is able to obtain O3 readings very close to the ground truth O3 level despite 30% participants are untrustworthy.

Keywords - Internet of Things; participatory sensing; trust; cloud computing.

1. Introduction

The physical world can be monitored by ubiquitous Internet of Things (IoT) devices through participatory sensing by which a huge amount of data is collected and analyzed for hazard detection and response. In this paper we present a case study of IoT participatory sensing [2, 4, 5] where IoT devices (e.g., smart phones carried by humans or smart cars driven by humans) can act as participants to collect air quality data and submit to a processing center located in the cloud for environmental data analysis. It is especially applicable to a health IoT group [8] where the main concern is about a pollutant (O3 in our case study). Users in the group report their O3 sensing results upon receiving a query from a member who wishes to find out a location's O3 level at a particular time to decide if it should enter the location based on its susceptibility to the O3 level detected.

The major challenge in IoT cloud participatory sensing is the selection of trustworthy participants because not all IoT devices will be trustworthy and some IoT devices may behave maliciously to disrupt the network or service (e.g., in a terrorist attack scenario) or just for their own gain (e.g., in an evacuation scenario following a disaster). We leverage a "Trust as a Service" (TaaS) cloud utility [1] to addresses the issue of selecting trustworthy participants. We compare the performance of TaaS against two contemporary trust protocols, Adaptive IoT Trust [3] and ObjectiveTrust [7] in selecting trustworthy participants. We show that TaaS can provide better performance than these contemporary IoT trust protocols. Using real traces of O3 levels and mobility traces of users in the O3 community of interest (O3COI) group in the city of Houston [10], we demonstrate that with the help of the TaaS cloud utility, a user in this O3COI group is able to obtain close to the ground truth O3 level.

The rest of the paper is organized as follows. In Section 2, we discuss the trace data used for the case study. In Section 3, we describe the background of trust-based IoT participatory sensing and the TaaS cloud utility used for selecting trustworthy participants for participatory sensing. We provide a brief literature survey to compare and contrast TaaS with existing distributed and centralized IoT trust protocols. We also provide the reason why we select two contemporary IoT trust protocols, namely, Adaptive IoT Trust [3] and ObjectiveTrust [7], for performance comparison. In Section 4, we conduct a performance analysis and compare the performance of TaaS against these two contemporary IoT trust protocols for selecting trustworthy participants for this case study. Finally Section 5 concludes the paper and outlines future work.

2. Trace Data Used for the Case Study

We use real traces of O3 levels and mobility traces of users in the O3 community of interest (O3COI) group in the city of Houston and apply it to our participatory sensing case study. The original dataset in [10] covers the socio-demographically relevant activity sequences and the movements of each individual in 4.9 million synthetic individuals in the Houston metropolitan area. We extract a portion of this huge database to cover a smaller set of members in the O3COI group along with their mobility and activity data around a smaller area. Figure 1 shows the synthetic individuals in the Houston metropolitan area and the zoomed view of a small region covering the locations of the target user. The coordinates in the figure represents the longitude and latitude of each synthetic individual. The zoomed area is divided into 8x8 regions. The red curve in the zoomed area represents the mobility of the target user. In the case study, we assume a percentage of nodes, denoted by P_M in the range of [0, 30%], are malicious. Every day this "good" member issues queries to its home cloud server before it enters a particular location to know the O3 level in the location it is about to step into. After collecting a number of O3 reports from other members, it then performs a trust-weighted computation to deduce the O3 reading (described later in Section 4). If the O3 level is below a threshold, it would follow its route; otherwise, it will not enter the location or it will detour to avoid the location because the location has a high O3 level that can harm its owner's health. After the query-and-response event is completed, this "good" member will assess if an O3 sensing report

submitted by another member is satisfactory and will submit the service experience to its home server so as to facilitate the implementation of the TaaS cloud utility (described later in Section 3).

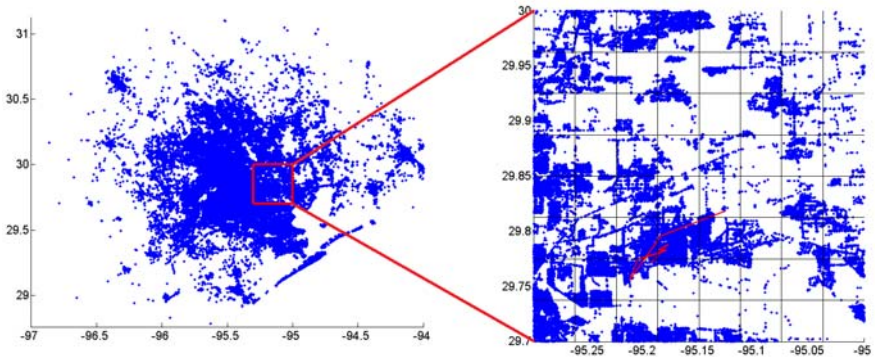

Figure 1: A zoomed view of a small region covering the locations visited by a target user in two days.

The Houston area has an extensive air monitoring network including 47 monitors measuring ozone. The O3 sensing data are not released in real time, but on an hourly basis. For our case study, hourly readings of ozone concentration levels (O3 ug/m^3 hourly) across 39 monitors in the Houston metropolitan area are used and served as "ground truth" against which a node's O3 sensing report is checked for service quality and the service experience is reported to the cloud server for TaaS service management.

3. Trust to Filter Untrustworthy Sensing Reports

The major challenge in IoT participatory sensing is the selection of trustworthy participants for aggregating sensing results [2, 4, 5]. In this section, we first describe our approach, leveraging the TaaS cloud utility [1] to filter untrustworthy sensing reports. Then we conduct a brief literature survey to compare and contrast TaaS with existing distributed and centralized IoT trust protocols.

3.1. Trust as a Service Cloud Utility

TaaS [1] is characterized by a simple report-and-query paradigm as follows:

- ***Reporting:*** Every user has a home cloud server. Whenever an O3 sensing report is provided by an IoT device, a user will report to its home cloud server whether it is satisfied with the service provided by this IoT device via a service rating report. Specifically, the user satisfaction experience of user u_x toward device d_i (belonging to a particular user) is assessed based on the difference between the actual or ground truth O3 reading (which is known to $u_x$after fact) and the O3 reading provided by device d_i.The user satisfaction experience denoted by s_i can be a real number in the range of 0 to 1 indicating the user satisfaction level, or simply a binary value, with 1 indicating satisfied and 0 not satisfied. A timestamp is also sent in the report to indicate the time at which this service rating happens. This allows cloud servers to know the event occurrence times of reports for regression analysis if necessary. Here s_i is the first piece of information sent from u_x to the home cloud server. The second piece of information sent from u_x to the home cloud server is its similarity score with u_y in terms of friendship, social contact, and community of interest, i.e., $sim_i(u_x, u_y),\ i \in \{f, s, c\}$. Upon receiving these similarity scores, $u_x's$ home cloud server uses a weighted sum formula $sim(u_x, u_y) = \sum_{i\in\{f,s,c\}} w_i \cdot sim_i(u_x, u_y)$ to compute the overall similarity score between u_x and u_y. The weights assigned to $sim_i(u_x, u_y),\ i \in \{f, s, c\}$, depend on the application characteristics and the designer's belief of what similarity metric is more important than others in composing the overall similarity score between two users. If both u_x and u_y are in the O3COI group then the community of interest similarity can be 1 and the weight on community of interest can be higher than those for friendship and social contact, if justified. In this case study, we consider equal weight, i.e., 1/3 for each weight.
- ***Querying*:** Whenever a user wants to know the trust value of an IoT device, it simply sends a query to its home cloud server. Let the "subjective" trust value of user u_x toward d_i (owned by another user) be denoted by $t_{x,i}$. The home cloud server of u_x computes $t_{x,i}$ by combining $u_x's$ direct trust toward d_i ($t_{x,i}^d$) based on own service ratings, and $u_x's$ indirect trust toward d_i ($t_{x,i}^r$) based on other users' service ratings, as follows:

$$t_{x,i} = \mu_{x,i} \cdot t_{x,i}^{d} + (1 - \mu_{x,i}) \cdot t_{x,i}^{r} \quad (1)$$

Here, $\mu_{x,i}$ is a weight parameter ($0 \leq \mu \leq 1$) to weigh the importance of direct trust relative to indirect trust. To cope with malicious attacks, the home cloud server of u_x dynamically controls $\mu_{x,i}$ in Equation 1 to weigh the importance of direct trust $t_{x,i}^{d}$ relative to indirect trust $t_{x,i}^{r}$ so as to minimize trust bias. The home cloud server of u_x applies adaptive filtering techniques [3] to control $\mu_{x,i}$. The direct trust $t_{x,i}^{d}$ in Equation 1 is computed by Beta Reputation [6] under which the trust value is modeled as a random variable in the range of [0, 1] following the Beta (α, β) distribution, and $t_{x,i}^{d} = \alpha/(\alpha + \beta)$ is the mean "direct" trust where α is the number of positive service experiences and is updated by $\alpha = \alpha + f_i$, and β is the number of negative service experiences and is updated by $\beta = \beta + (1 - f_i)$ upon receiving a service rating f_i from user u_x about $d_i's$ service quality after d_i completes a service for u_x. The indirect trust $t_{x,i}^{r}$ in Equation 1 is computed by the home cloud server of u_x by first locating all social similarity records $sim(u_x, u_y)'s$ in its local storage. The home cloud server of u_x then selects top-R raters from R users with the highest similarity scores with u_x and calculates the indirect trust ($t_{x,i}^{r}$) towards device d_i as follows:

$$t_{x,i}^{r} = \sum_{u_y \in U} \frac{sim(u_x, u_y)}{\sum_{u_z \in U} sim(u_x, u_z)} \cdot t_{y,i}^{d} \quad (2)$$

Here, U is a set of up to R raters whose $sim(u_x, u_y)$ scores are the highest, $u_y \in U$ is a rater selected, and $t_{y,i}^{d}$ is the service rating provided by u_y toward device d_i. We note that $t_{y,i}^{d}$ is stored in the home cloud server of u_y but it is obtainable after the home cloud server of u_x communicates with the home cloud server of u_y. In Equation 2, the service rating provided from u_y toward d_i $(\text{i.e.}, t_{y,i}^{d})$ is weighted by the ratio of the similarity score of u_x toward u_y to the sum of the similarity scores toward all raters. If the overall similarity score of u_x toward u_y is high relative to that of u_x toward other raters, then the home cloud server of u_x will put a relatively high weight on the service rating $t_{y,i}^{d}$ provided by u_y to compute $t_{x,i}^{r}$.

3.2. IoT Trust Protocols

Our approach to trust-based IoT participatory sensing of air quality is based on integrating cloud service with trust management service to create an IoT service-community cloud utility, aka, Trust as a Service (TaaS), for centralized or hierarchically structured IoT systems [1, 28]. An IoT service-community can be an e-health group (as considered in this paper) paying particular attention to air pollution for the welfare of a group of users who may suffer from polluted air quality, an intelligent your-ride-on-demand IoT group (like Uber), or a smart city group consisting of visitors, merchants, restaurants, and entertainment business entities, etc. TaaS thus is a service provided by the cloud to members in each of these groups. Service feedback along with service context information can be fed into the cloud for a complete statistical analysis. Users requesting a service or a composite service (i.e., several services bundled together via service composition and binding) can be assured of trustworthy, high-quality service, as a result of TaaS being applied to a service-community group. Here we note that the issue of making the TaaS cloud utility more reconfigurable, fault-tolerant, scalable, or resilient to a large number of IoT devices as well as cloud and network failure [12-17, 21-24, 28] is outside the scope of this paper. In this paper, we focus on TaaS being applied to an IoT e-health service-community specifically interested in ozone air quality.

Trust management protocols for IoT systems are still emerging. There are only a handful of IoT trust protocols designed and evaluated to-date [1, 3, 7-9, 25-28]. Among the contemporary IoT trust management protocols, we select two very recent ones, namely, Adaptive IoT Trust [3] and ObjectiveTrust [7] as baseline IoT trust protocols against which TaaS is compared for performance analysis.

The reason we select Adaptive IoT Trust [3] is that it, like TaaS, also considers adaptive trust management to dynamically combine own experiences with recommendation based on the amount of own experiences in hand (as described in Equation 1) and uses social similarity for recommendation filtering (as described in Equation 2). Also, it was shown in [3] that Adaptive IoT Trust outperforms existing distributed P2P trust protocols, including EigenTrust [18], PeerTrust [19], and ServiceTrust [20], so we are interested in knowing if TaaS, a cloud-based IoT trust protocol, can perform better than Adaptive IoT Trust, a proven distributed IoT trust protocol. The reason we select ObjectiveTrust [7] is that it is the only other centralized IoT trust

protocol to-date that considers social standing and relationships for credibility rating and recommendation filtering.

Below we provide an overview of the two baseline IoT trust protocols and compare and contrast them with TaaS.

Adaptive IoT Trust [3] is a distributed IoT trust management protocol where each IoT device evaluates other IoT devices using both direct service experiences and indirect recommendations. Adaptive trust management is achieved by determining the best way to combine direct trust (from direct experiences) and indirect trust (from recommendations) dynamically to minimize convergence time and trust estimation bias in the presence of malicious nodes performing collusion attacks. Direct service experiences are collected based on own service experiences, while recommendations are collected at the time nodes encounter each other through social contacts. They used social similarity to rate recommenders. A common problem with a distributed IoT trust protocol such as Adaptive IoT Trust [3] is that a node may not encounter each other often to collect enough recommendations to make informed decisions. Also all trust data are stored by individual IoT devices, which can be a problem for resource-constrained IoT devices, especially when the number of IoT devices is high in a large-scale IoT system. Our approach based on TaaS does not have such constraints.

ObjectiveTrust [7] is a centralized IoT trust management system that assesses the trust score of a node through a weighted sum of the "centrality" score and the average opinion score (long term and short term) after applying the recommender's credibility score to filter untrustworthy recommendations. Specifically, ObjectiveTrust computes the centrality score (in the range of 0 to 1) of *j* based on if *j i*s central in the network and if it is involved in many transactions. The credibility score of *k* (a recommender that provides opinions about *i)* is proportional to *k*'s trust score because a trustworthy node does not lie, but is inversely proportional to the capability of *k,* the strong object relationship (including ownership, co-location, co-work, social, and parental) between *i* and *k*, and the number of transactions between *i* and *k* because high-capability and intimate nodes may collude. A common problem of a centralized IoT trust protocol such as ObjectiveTrust [7] is that it only computes the "objective trust" (common belief or reputation), not the "subjective trust" of an IoT device as TaaS and Adaptive IoT Trust do, so it does not preserve the notion that trust is subjective and is inherently one-to-one. This is especially problematic for IoT systems since IoT

devices are owned by humans who have social relationships among themselves and the trust of one user toward another user is inherently one-to-one and subjective.

4. Results

In this section, we present our case study results. Our case study is a health IoT application used by O3COI group members whose daily mobility and activity levels are composed from real traces as discussed in Section 2.

4.1. Trust-based IoT Participatory Sensing of O3

A node (node *i*) in the O3COI group can query the ozone level in a particular location and at a particular time via a mobile IoT cloud application [8, 11] installed in its smartphone. The mobile application would send the query to all O3COI members that are in this particular location via the mobile cloud application. Upon receiving O3 sensing reports from other members, node *i* sends queries via TaaS to get the trustworthiness scores of these IoT devices who had reported sensing reports. To filter out untrustworthy O3 sensing reports, node *i* first accepts a sensing report (S_j) from *j* only if *j* is deemed trustworthy for O3 sensing service (i.e., *i*'s trust score toward *j*, t_{ij}, is higher than 0.5 as determined by TaaS by Equation 1). Then it computes a trust-weighted O3 level average as follows:

$$S = \sum_{j=1}^{N} (t_{ij} / \sum_{j=1}^{N} t_{ij}) \times S_j. \quad (3)$$

where *N* is the number of trustworthy members providing O3 sensing reports in the particular location. If the average O3 level exceeds a maximum threshold defined by *i*'s owner, node *i* will decide not to visit the location because the ozone level will cause harm to its owner's health. Figure 2 shows a scenario in which the target node (node *i*) before moving to a new location asks for the ozone level through trust-based participatory sensing. In this scenario, *j* and *k* provide O3 levels 180 and 40, respectively. However since *j*'s trust score is only 0.2 (supplied by TaaS), the O3 level reported by *j* (180) is filtered out. Node *k*'s trust score is 0.9 (supplied by TaaS), so the O3 level (40) reported by *k* is accepted. Node *i* then applies Equation 3 to compute the average O3 level. Since the average O3 level is below the maximum threshold, node

i decides to step into the location. Node *i* later checks the ground truth O3 level against sensing readings reported by *j* and *k*. As a result, node *i* reports a positive service rating for *k* because *k* provided a satisfactory O3 level, but a negative service rating against *j* because of the large discrepancy between the ground truth O3 level and the high O3 level reported by *j*.

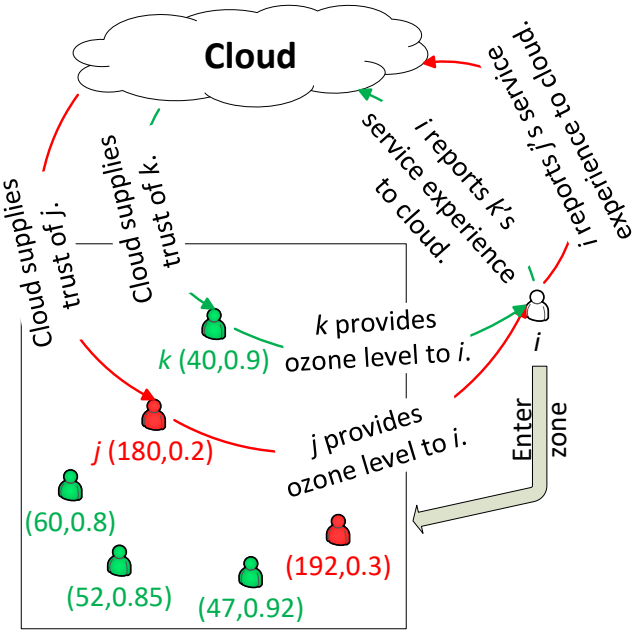

Figure 2: A scenario illustrating how a target node acts in the trust-based participatory sensing application before moving to a new location.

4.2. Experimental Setup

Using the ns3 simulator, we simulate the participatory sensing system. We use real traces of O3 levels and mobility traces of users in the O3COI group in the city of Houston [10]. A user follows its mobility pattern while performing the report-and-query paradigm to query the O3 level in a new location it steps into as well as report its user satisfaction experience and similarity score with another node it encounters, as discussed in Section 3. The O3 level can be classified as in good condition (below 50 ug/m^3), medium condition (between 51 and 168 ug/m^3) for unhealthy for sensitive groups, poor condition (between 169 and 208 ug/m^3), and severe condition (above 209 ug/m^3).

The percentage of bad nodes is set at P_M in the range of 0% to 30%. A malicious node always reports O3 readings in the poor condition range (between 169 and 208 ug/m^3) regardless of location with the intention to break the system.

A malicious node also performs bad-mouthing attacks (saying a good node's sensing result is not trustworthy in the user satisfaction report) and ballot-stuffing attacks (saying a bad node's sensing result is trustworthy) when it submits a service rating report recording its satisfaction experience s_i toward device d_i. Specifically, a malicious IoT device provides a user satisfaction score of 0 against a good IoT device for bad-mouthing attacks, and conversely a user satisfaction score of 1 for a malicious device for ballot-stuffing attacks. TaaS handles ballot-stuffing and bad-mouthing attacks by means of social similarity based recommendation filtering, i.e., based on Equations 1, 2, and 3.

4.3. Performance Evaluation

We measure two performance metrics for performance evaluation:

- The trust-weighted average O3 reading vs. ground truth (i.e., the actual O3 level at a specific location and a particular time).
- The accuracy of selecting trustworthy participants.

The goal is to prove that TaaS provides O3 readings close to ground truth and can perform better than existing IoT trust protocols.

We first conduct a performance evaluation of TaaS against contemporary distributed IoT trust protocols, including EigenTrust [18], PeerTrust [19], ServiceTrust [20], and Adaptive IoT Trust [3] for which each IoT device keeps own trust data based on own experiences and service satisfaction ratings from peers that it encounters.

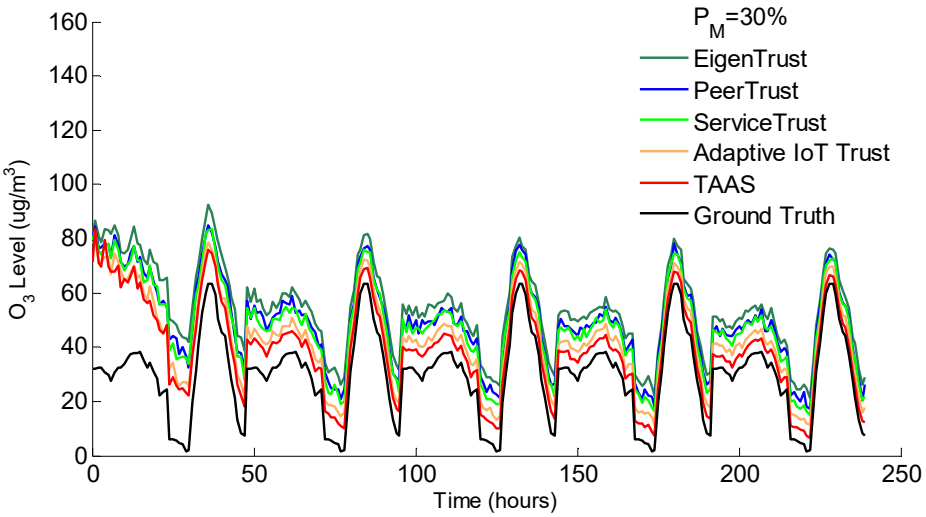

Figure 3: Performance comparison of TaaS against distributed IoT trust protocols in the trust-weighted average O3 reading.

Figure 3 shows the trust-weighted average O3 readings vs. time of a selected target node (each time point is an O3 query service request) with the percentage of bad nodes P_M set at 30%. In the experiment, the target node repeatedly queries the ozone level in the location that he will visit next over a 250 hour span. Each data point under a particular trust protocol is the average O3 level obtained from Equation 3. For example, at time t = 10 hours, the target node sends queries via TaaS to get the trustworthiness scores of those IoT devices that have supplied O3 readings in the particular location. The target node accepts results (S_j) from 557 trustworthy IoT devices (for which the trust score is higher than 0.5) for the O3 sensing service out of all 764 members in that particular location at that particular time and it then computes the average O3 level based on Equation 3.

The results indicate that TaaS (red line) can provide O3 readings very close to ground truth (black line) as time progresses. Further, TaaS outperforms EigenTrust, PeerTrust, ServiceTrust, and Adaptive IoT Trust in terms of accuracy (i.e., the difference between ground truth and the average O3 levels), convergence (i.e., the speed at which the average O3 level curve approaches the ground truth curve), and resiliency (against malicious attacks of 30% bad nodes) due to its ability to

effectively aggregate trust evidence from all nodes in the system through our effective and efficient localized report-and-query paradigm.

Figure 4 shows the percentage of bad nodes selected to provide sensing results of a selected target node. TaaS outperforms EigenTrust, PeerTrust, ServiceTrust, and Adaptive IoT Trust as time progresses because TaaS is not being limited by encountering experiences and can leverage cloud service to aggregate broad evidence from all nodes who have had sensing service experiences with a target IoT device.

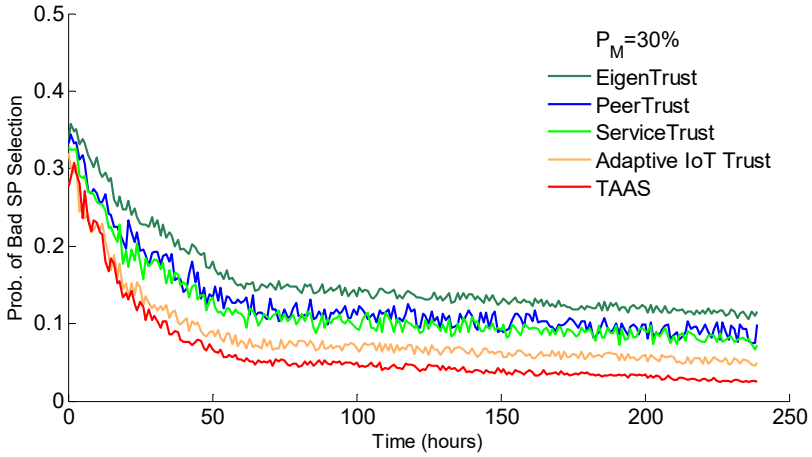

Figure 4: Performance comparison of TaaS against distributed IoT trust protocols in the percentage of bad IoT devices selected to provide O3 sensing service.

Next we compare TaaS with a contemporary centralized IoT trust protocol, ObjectiveTrust [7]. From Figures 3 and 4, we know Adaptive IoT Trust [3] provides the best performance among existing distributed IoT trust protocols. Therefore, in the performance analysis below, we also include Adaptive IoT Trust [3] for performance comparison.

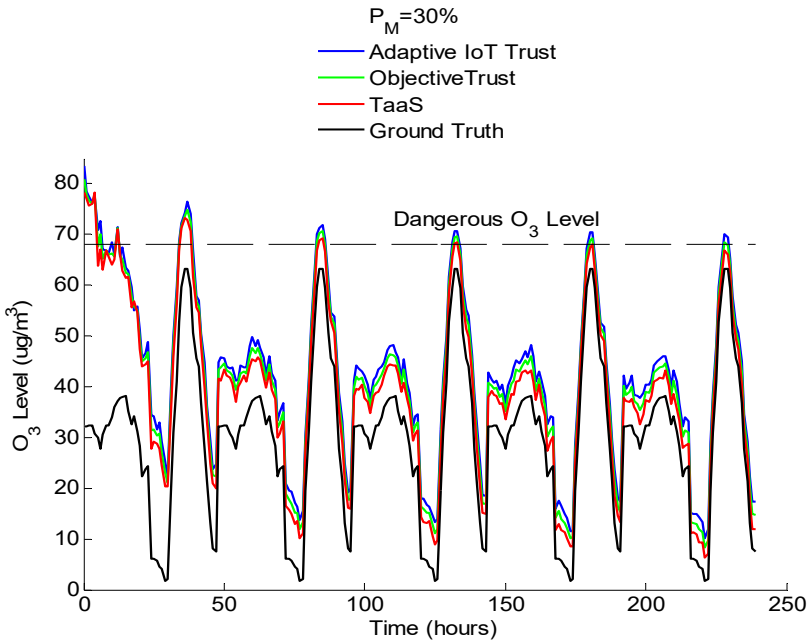

Figure 5: Performance Comparison of Trust-Weighted Average O3 Readings.

Figure 5 shows the trust-weighted average O3 readings vs. time of a target node randomly selected (again each time point is an O3 detection service request) with the percentage of bad nodes P_M set at 30%. Similar to Figure 3 we again observe that TaaS (red line) can provide O3 readings very close to ground truth (black line) as time progresses. TaaS outperforms Adaptive IoT Trust (orange line) and ObjectiveTrust (green line) in terms of accuracy (i.e., the difference between ground truth and the average O3 levels) and resiliency (against malicious attacks of 30% bad nodes). We draw a line "Dangerous O3 Level" for a user whose "dangerous O3 level" is 68 as diagnosed by his/her doctor as vulnerable to O3 exposure for more than 4 hours. We see that at time t=130, 180, or 235 (the last three peaks in the figure) only TaaS will correctly identify the fact that O3 level is below the dangerous level, while either Adaptive IoT Trust or ObjectiveTrust will raise a false alarm that the dangerous O3 level for this user is already reached.

Figure 6 shows the percentage of bad nodes selected to provide sensing results to a selected target node. TaaS again outperforms Adaptive IoT Trust and ObjectiveTrust as time progresses. The results can be explained as follows: Compared with Adaptive IoT Trust, TaaS is not being limited by encountering experiences and can leverage cloud service to aggregate broad evidence from all nodes who have had sensing service experiences with a target IoT device. Compared with ObjectiveTrust which is based on "objective trust" (i.e., common belief), TaaS is based on "subjective trust" (one-to-one trust evaluation) and can adaptively put a higher weight on a participant if it has had good O3 sensing experiences with the particular participant. This allows TaaS to more effectively select trustworthy participants among all participants that had submitted O3 sensing reports.

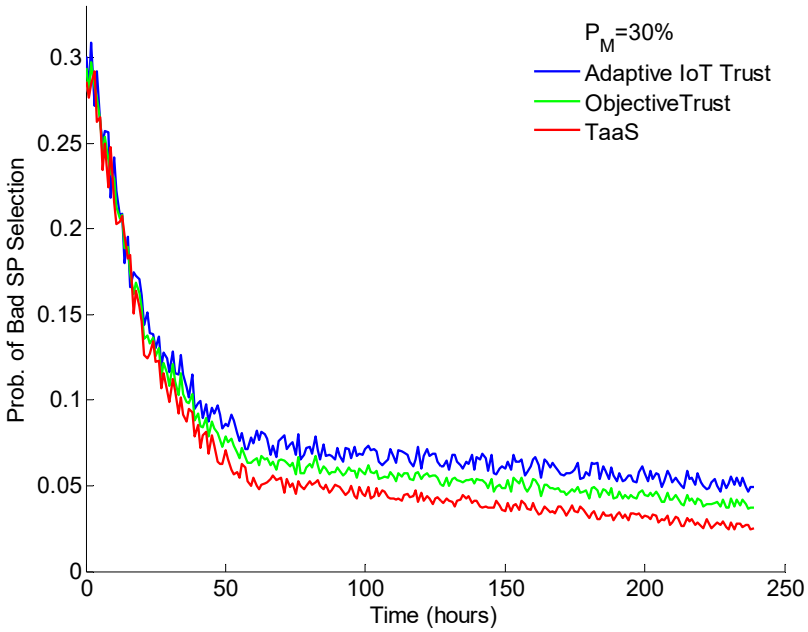

Figure 6: Percentage of Bad IoT Devices Selected to Provide O3 Sensing Service.

5. Conclusion

In this paper we conducted trust-based IoT participatory sensing of air quality using ozone and user mobility traces. We demonstrated that

by leveraging the TaaS cloud utility, a user can obtain ozone readings close to the ground truth readings. The main reason is that TaaS can effectively filter untrustworthy sensing reports from users who are not trustworthy, i.e., having a low trust value in ozone sensing service based on past history collected in the cloud for the O3 health group. Also TaaS outperforms contemporary distributed and centralized IoT trust protocols in the case study using real traces. We attribute the effectiveness to the TaaS cloud utility to its ability to adaptively and effectively combine own experiences and trust evidence from a broad set of IoT participants who have had experiences with a target IoT device in O3 sensing service, thus allowing a user to be able to accurately assess if a target IoT device providing O3 sensing service is trustworthy or not. In the future, we plan to conduct more experiments to quantify the gain of our design in terms of performance metrics such as resource overhead, energy consumption, and service latency.

Acknowledgement

This work is supported in part by the U.S. AFOSR under grant number FA2386-17-1-4076.

References

[1] I.R. Chen, J. Guo, and J.J.P. Tsai, "Trust as a Service for SOA-based Internet of Things," *Services Transactions on Internet of Things,* vol. 1, no. 1, 2017, pp. 43-52.

[2] W.Z. Khan, Y. Xiang, M.Y. Aalsalem, and Q. Arshad, Q, "Mobile Phone Sensing Systems: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, 2013, pp. 402–427.

[3] I.R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-based IoT and Its Application to Service Composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, 2016, pp. 482-495.

[4] H. Mousa, et al. "Trust Management and Reputations Systems in Mobile Participatory Sensing Applications: A Survey," *Computer Networks*, vol. 90, 2015, pp. 49-73.

[5] H. Amintoosi, S.S. Kanhere, and M. Allahbakhsh, "Trust-based Privacy-aware Participant Selection in Social Participatory Sensing," *J. Information Security and Applications*, vol. 20, 2015, pp. 11-25.

[6] A. Jøsang, and R. Ismail, "The Beta Reputation System," *Bled Electronic Commerce Conference*, Bled, Slovenia, 2002, pp. 1-14.

[7] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness Management in the Social Internet of Things," *IEEE Transactions on Knowledge and Data Management*, vol. 26, no. 5, 2014, pp. 1253-1266.

[8] H. Al-Hamadi and I.R. Chen, “Trust-Based Decision Making for Health IoT Systems,” *IEEE Internet of Things Journal*, vol. 4, no. 5, Oct. 2017, pp. 1408-1419.
[9] J. Guo, I. R. Chen, and J.J.P. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications,* vol. 97, 2017, pp. 1-14.
[10] B. Pires, et al, “Towards an in silico Experimental Platform for Air Quality: Houston, TX as a Case Study,” *Computational Social Science Society of America Conference*, Santa Fe, NM, USA, 2015.
[11] Y. Wang, I.R. Chen, and D.C. Wang, “A Survey of Mobile Cloud Computing Applications: Perspectives and Challenges,” *Wireless Personal Communications*, vol. 80, 2015, pp. 1607-1623.
[12] I.R. Chen, B. Gu, S.E. George, and S.T. Cheng, “On failure recoverability of client-server applications in mobile wireless environments,” *IEEE Trans. Reliability*, vol. 54, no. 1, 2005, pp. 115-122.
[13] B. Gu and I. R. Chen, “Performance analysis of location-aware mobile service proxies for reducing network cost in personal communication systems,” *Mobile Networks and Applications,* vol. 10, no. 4, 2005, pp. 453-463.
[14] S.T. Cheng, C.M. Chen, and I.R. Chen, “Dynamic quota-based admission control with sub-rating in multimedia servers,” *Multimedia Systems*, vol. 8, no. 2, 2000, pp. 83-91.
[15] S.T. Cheng, C.M. Chen, and I.R. Chen, “Performance evaluation of an admission control algorithm: dynamic threshold with negotiations,” *Performance Evaluation*, vol. 52, no. 1, 2003, pp. 1-13.
[16] O. Yilmaz and I.R. Chen, "Utilizing Call Admission Control for Pricing Optimization of Multiple Service Classes in Wireless Cellular Networks," *Computer Communications*, vol. 32, no. 2, 2009, pp. 317-323.
[17] I. R. Chen, T.M. Chen, and C. Lee, “Agent-based forwarding strategies for reducing location management cost in mobile networks,” *Mobile Networks and Applications*, vol. 6, no. 2, 2001, pp. 105-115.
[18] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, “The EigenTrust Algorithm for Reputation Management in P2P Networks,” *12th International Conference on World Wide Web*, Budapest, Hungary, 2003.
[19] L. Xiong, and L. Liu, “PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities,” *IEEE Trans. on Knowledge and Data Engineering* 16, pp. 843-857, 2004.
[20] Z. Su, L. Liu, M. Li, X. Fan, and Y. Zhou, “ServiceTrust: Trust Management in Service Provision Networks,” *IEEE International Conf. on Services Computing,* Santa Clara, CA, USA, 2013, pp. 272-279.
[21] I.R. Chen and D.C. Wang, “Analysis of Replicated Data with Repair Dependency,” *The Computer Journal*, vol. 39, no. 9, 1996, pp. 767-779.
[22] I.R. Chen, O. Yilmaz, and I.L. Yen, "Admission control algorithms for revenue optimization with QoS guarantees in mobile wireless networks," *Wireless Personal Communications*, vol. 38, no. 3, 2006, pp. 357-376.
[23] I.R. Chen and F.B. Bastani, "Effect of Artificial-Intelligence Planning Procedures on System Reliability," *IEEE Trans Reliability*, vol. 40, no. 3, pp. 364-369, 1991.
[24] I.R. Chen, J. Guo, F. Bao and J.H. Cho, “Trust Management in Mobile Ad Hoc Networks for Bias Minimization and Application Performance Maximization,” *Ad Hoc Networks*, vol. 19, August 2014, pp. 59-74.

[25] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, “Trust management system design for the Internet of Things: A context-aware and multi-service approach,” *Computers and Security*, vol. 39, Nov. 2013, pp. 351-365.

[26] I. R. Chen, F. Bao, and J. Guo, "Trust-based Service Management for Social Internet of Things Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, Nov-Dec 2016, pp. 684-696.

[27] M. Nitti, L. Atzori, and I.P. Cvijikj, “Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies,” *IEEE Internet of Things Journal*, vol. 2, no. 3, 2015, pp. 240-247.

[28] J. Guo, I.R. Chen, and J.J.P. Tsai, “A Mobile Cloud Hierarchical Trust Management Protocol for IoT Systems,” *5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, San Francisco, April 2017.