MASA: Multi-agent Subjectivity Alignment for Trustworthy Internet of Things

Leonit Zeynalvand, Jie Zhang, Tony T. Luo†, Shuo Chen
School of Computer Science and Engineering, Nanyang Technological University, Singapore
†*Institute for Infocomm Research, Agency for Science, Technology and Research (A*STAR)*, Singapore
Leonit001@e.ntu.edu.sg, zhangj@ntu.edu.sg, luot@i2r.a-star.edu.sg, chen1087@e.ntu.edu.sg

***Abstract*—The vastly diverse and increasingly autonomous Internet of Things (IoT) devices stress trust management as a critical requirement of IoT. This paper addresses subjectivity as an important issue in trust management for IoT. Subjectivity means that the information provided by each autonomous IoT device, represented by an agent, is likely to have been influenced by the device's individual preference, which can be misleading in trust evaluation. In this paper, we seek to align the potentially subjective information with the information seeker's own subjectivity so that the acquired second-hand information is more useful and personalized. Accordingly, we propose a multi-agent subjectivity alignment (MASA) mechanism, which models the subjectivity using a regression technique and exchanges the models among agents as the input to an alignment process. This mechanism substantially counteracts biases incurred by different agents and improves the accuracy of second-hand information fusion as demonstrated by our simulations. In addition, we also conduct experiments using a real-world dataset (MovieLens) which further validates the efficacy of MASA.**

***Index Terms*—Trust, Subjectivity, IoT**

I. Introduction

The Internet of Things (IoT) opened the doors for smart interconnected devices to be engaged in autonomous exchange of information and services. While IoT applications are compelling, IoT devices may not be trustworthy which can hinder the realization of these applications. Therefore, trust plays an important role in IoT. Computational trust systems generally calculate trust values based on two types of data: first-hand evidence (experiences of self) and second-hand evidence (advice from others). With the prevalence of IoT and growing number of devices, the first-hand evidence space has become too sparse to suffice for reliable trust calculations. Hence, the reliance on second-hand evidence has become more prominent.

However, second-hand evidence often suffers from high subjectivity in IoT. Specifically, IoT involves highly heterogeneous devices such as smart cars, phones and wearables which have different capabilities and limitations. This heterogeneity leads to different criteria for the agents that represent the devices to evaluate their interaction outcomes, resulting in highly subjective second-hand evidence in IoT.

To further clarify what we mean by subjectivity, let us first consider an analogy where Alice has high tolerance for spicy food while Bob's tolerance for spicy food is low. Hence, whenever Alice advises Bob that a certain dish is *slightly spicy*, it is probably of Bob's best interest to avoid the dish. To frame the same concept under a crowd-sensing example in smart transportation domain, let us consider agents A and B which respectively represent a smart car and a smart phone. Agent A has a speed sensor precision of $1mph$, while agent B has a precision of $5mph$. So agent B will consider any crowd-sensed measurement which deviates less than $5mph$ from its belief of ground truth as *truthful* while agent A may consider the same measurement as *not truthful*. These two simple examples reflect the issue that we refer to as subjectivity in this paper.

Despite the vast literature on trust and reputation management systems [1], the issue of subjectivity in trust has not been well addressed. A few recent studies made an attempt to address subjectivity, but their restrictive assumptions do not fit IoT domain well. Fang et al. [2] assumed strong naive independence between the attributes that influence the subjectivity which does not hold for IoT applications (e.g. knowing that a phone has a low resolution camera implies an old model and hence decreases the odds for it to have a near-field communication sensor). Clustering is used in [3] to group similar-thinking users together based on their provided ratings. However, it dictates a centralized approach which is not realistic for decentralized IoT applications.

In this paper, we propose a multi-agent subjectivity alignment (MASA) mechanism, in which the process of how each agent evaluates the outcome of its interactions with other agents, is modeled by a regression technique. The models are then exchanged when agents offer advice (referred to as second-hand evidence) to each other, followed by an alignment process. This alignment mechanism substantially counteracts biases incurred by other agents (Section II-A). Each aligned advice then is propagated to the underlying trust and reputation management system to be fused with the rest of second-hand evidence using uncertainty-aware weights which are computed with our proposed method (Section II-B). This improves the accuracy of the second-hand evidence fusion. A running example of the entire process is provided in Section III.

We make the following contributions in this paper.

- We propose MASA which can be seamlessly incorporated into existing trust and reputation management systems as a plugin.
- We demonstrate the effectiveness of MASA by conducting simulations for two different scenarios. First, we simulate the scenario of Internet data plan sharing in a smart city context (section IV-A). Second, we simulate an

978-0-9964527-7-9 ©2018 ISIF

IoT-based crowd-sensing application in the transportation domain (section IV-B).
- We apply MASA to real data obtained from MovieLens dataset [4]. The results further validate the efficacy of MASA and indicate that MASA can also be applied to other domains besides IoT (section IV-C).

II. MASA

Computational trust systems generally calculate trust scores based on two types of data: first-hand evidence (self experiences) and second-hand evidence (advice). We refer to an agent who offers second-hand evidence as $advisor$ and an agent who requests second-hand evidence as $advisee$. An agent can be an advisor, an advisee, or both. Each request by an agent for a specific information/service together with the response from the other agent, is called an interaction and can have several features (e.g. response time, latency, etc.). In the rest of this paper, the process of how each agent evaluates the outcome of its interaction with another agent is referred to as interaction outcome evaluation (IOE). The inputs of IOE are interaction features and the output is a first-hand evidence. In MASA, the IOE of each agent is modelled using decision tree regression, where the inputs of IOE are used as the feature set and the output is used as the dependent variable to train the model. We use the classification and regression tree (CART) algorithm [5] to build the decision trees. The agents then exchange these models when offering advice to each other, followed by an alignment process (Section II-A). Each aligned advice then is propagated to the underlying trust and reputation management system to be fused with the rest of the second-hand evidence using uncertainty-aware weights which are computed with our proposed entropy-base method (Section II-B). This improves the accuracy of second-hand evidence fusion. Finally (Section II-C), we explain the rationale why we use decision tree regression as our design choice.

A. Advice Alignment

We denote the decision tree which represents an agent's IOE as T. The global set of interaction features (IOE inputs) used by agents to train their decision trees is denoted by $F = \{f_1, f_2, ...\}$ (e.g. response time, error rate, delay, etc.). The set of distinct leaves in the decision tree of agent i, or in other words the set of possible outputs of agent i's IOE, (e.g. excellent, good, fair, bad, etc.) is denoted as $D_i = \{d_{i1}, d_{i2}, ...\}$. Categorical values will be converted to numeric form as $\tilde{D}_i = \{1, 2, ..., |D_i|\}$ with order maintained. The set of paths (rules) in the corresponding decision tree T for agent i from the root to the leaves with a value equal to $j \in \tilde{D}_i$ is denoted as $R^{Tj} = \{r_k^{Tj} | k = 1, 2, ...\}$ and the set of decision nodes in rule k is denoted as $C(r_k^{Tj}) = \{c_t | t = 1, 2, ...\}$ where c_t is a condition over a specific $f \in F$ (e.g. $error < 5mph$). Finally, the condition set, i.e. the conjunction of all $c_t \in C(r_k^{Tj})$ is denoted as $\tilde{C}(r_k^{Tj}) = (c_1 \cap c_2 \cap ...)$.

In MASA, whenever an advisor agent i offers an advice $x \in \tilde{D}_i$ to advisee agent i', it also offers T. Having x and T, for each outcome $j \in \tilde{D}_{i'}$, advisee can compute the posterior probability that j could be observed by itself given that outcome x has been observed by advisor i. Following Algorithm 1,[1] posterior probability is calculated as follows:

$$p(T'(j)|T(x)) = \frac{|\bigcup_{n=1}^{|R^{T'j}|} \tilde{C}(r_n^{T'j}) \cap \bigcup_{m=1}^{|R^{Tx}|} \tilde{C}(r_m^{Tx})|}{|\bigcup_{m=1}^{|R^{Tx}|} \tilde{C}(r_m^{Tx})|} \quad (1)$$

Here, given advice x and advisor's decision tree T as input, the denominator in Eqn. 1 is obtained by traversing T from the root to leaf node(s) with a value equal to x (lines 2-6). In each traverse, logical conjunction is performed on all $c_i \in C(r_m^{Tx})$ or in other words all the vertices in each path from the root to the corresponding leaf node(s). Then, logical disjunction is performed on the results Set_x obtained from each path. The value of $Denominator$ (line 6) can be computed by counting the number of occurrences of B over a representative sample set of either the advisor's first-hand evidence, or a global first-hand evidence (e.g. maintained by a third party acting as an auditing centre). Intuitively both computation strategies would yield equivalent results under the assumption of no discrimination and given enough observations. However, the former is more prone to cold start. Moreover, to ensure privacy both sample sets can be anonymized since B carries no identity information.

Similarly (lines 7-11), the numerator of Eqn. 1 is obtained by also considering T' (the decision tree of the advisee). Finally, a probability vector in the form of $[p_1, p_2, ..., p_{|D_{i'}|}]$ is obtained from the calculated values of the posterior probabilities for all $j \in \tilde{D}_{i'}$ (lines 12-18). This probability vector represents the probability mass function of the subjectively aligned advice as a random variable. MASA passes the ex-

Algorithm 1 Advice Alignment Algorithm

Inputs: The advice x, the regression trees T of advisor and T' of advisee.
Output: $cpmf$ which is the probability vector of the random variable representing the aligned advice.

1: **procedure** TUNE(x, T, T')
2: **for** each decision path r_m^{Tx} in T **do**
3: $Set_x \xleftarrow{\text{add}} Conjunction\_of\_Elements(C(r_m^{Tx}))$
4: **end for**
5: $B \leftarrow Disjunction\_of\_Elements(Set_x)$
6: $Denominator \leftarrow count(B)$
7: **for** j in ratingRange **do** ▷ ($e.g.\ j \in \{1, 2, 3, ..., 10\}$)
8: **for** each decision path $r_n^{T'j}$ in T' **do**
9: $Set_j \xleftarrow{\text{add}} Conjunction\_of\_Elements(C(r_n^{T'j}))$
10: **end for**
11: **end for**
12: **for** j in ratingRange **do** ▷ ($e.g.\ j \in \{1, 2, 3, ..., 10\}$)
13: $Temp \leftarrow Disjunction\_of\_Elements(Set_j)$
14: $A \leftarrow Conjunction(Temp, B)$
15: $Numerator \leftarrow count(A)$
16: $cpmf[j] \leftarrow Numerator/Denominator$
17: **end for**
18: **return** $cpmf$ ▷ ($e.g.\ [p_1, p_2, ..., p_{10}]$)
19: **end procedure**

[1] A step-by-step example of the procedure is provided in Section III.

pected value of this random variable to the underlying trust and reputation system as the subjectively aligned advice together with a fusion weight calculated in the next section (II-B).

B. Variance-modulated Entropy

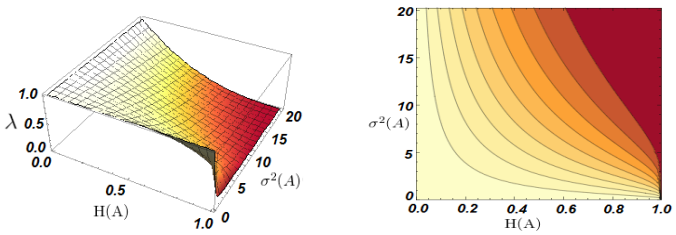
The probability distribution obtained by Algorithm 1 may carry little or no information representing the subjectively aligned advice (e.g. a discrete uniform distribution which means that all values in the advice range are equally likely to be observed). Hence, a measure is needed to capture how informative an advice is after being transformed into advisee's subjectivity domain. This measure can then be utilised to fuse the subjectively aligned advice with the rest of the second-hand evidence. In MASA, we propose such a measure by combining two metrics in probability theory and statistics: entropy and variance. While either metric partially indicates the amount of information embedded in the random variable representing the transformed advice, neither alone provides a robust measure. To clarify, consider four random variables with given probability vectors:

- $A_1 = [0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1, 0.1]$
- $A_2 = [0, 0, 0, 0, 0.01, 0.09, 0.1, 0.6, 0.1, 0.1]$
- $A_3 = [0.5, 0, 0, 0, 0, 0, 0, 0, 0, 0.5]$
- $A_4 = [0, 0, 0, 0, 0, 0, 0, 0, 0.5, 0.5]$

Each random variable represents a subjectively aligned advice. Entropy justifies picking A_2 over A_1 since the entropy of A_1 is equal to one which means the highest uncertainty, while A_2 has a much lower entropy. However, A_3 and A_4 have the same entropy while A_3 is not the better pick because of its high variance compared to A_4 (i.e. it is not clear the advice is 1 or 10 while in A_4 we are almost certain that the advice is somewhat around 9.5). This shows that entropy alone is not descriptive enough for our case. Hence, we define:

$$\lambda(A) = (1 - H(A))^{\frac{12\sigma^2(A)}{|\tilde{D}_{i'}|^2 - 1}} \tag{2}$$

which we refer to as *variance-modulated entropy* as a measure of how informative an advice is after being transformed into an advisee's subjectivity domain. In Eqn. 2, A is the random variable representing the transformed advice whose probability vector is calculated using Algorithm 1, $H(A)$ is the entropy of A, and $\tilde{D}_{i'}$ is the range of A. To clarify the rationale behind Eqn. 2, consider a random variable A' with discrete uniform distribution $U\{1, |\tilde{D}_{i'}|\}$. Since A' taking any of the values in its range is equally probable, the uncertainty in the aligned advice is maximum. Hence, we consider A' as the benchmark and compare A with that benchmark to derive $\lambda(A)$. Given its uniform distribution, $H(A')$ is equal to one. As a result, smaller values for $H(A)$ indicate more certainty as captured by the base of Eqn. 2. Similarly, $\sigma^2(A') = (|\tilde{D}_{i'}|^2 - 1)/12$. Hence, greater values of $\sigma^2(A)$ implies less certainty as captured by the exponent of Eqn. 2. As illustrated in Figure 1, the value of $\lambda(A)$ is always in range $[0, 1]$ where 1 indicates absolute certainty while 0 means complete uncertainty. Although not all the points on the surface in Figure 1 can be observed in practice since entropy and variance are not completely independent, it is not an issue for MASA as we are only interested in those that can be observed.



(a) (b)

Fig. 1: variance-modulated entropy for posterior advice random variable A with a range of $\{1, 2, ..., 10\}$. ($\sigma^2_{U\{1,10\}} = 20.25$) (a) 3D plot. (b) Contour plot.

Existing trust and reputation management systems [6], [7] often employ a weighted sum of second hand evidence in their fusion mechanisms to aggregate the advice received from different advisors. Hence, MASA propagates $\lambda(A)$ to the underlying trust system where it can be utilised as the weight to fuse the subjectively aligned advice with the second-hand evidence obtained from other agents.

C. Rationale of using Decision Trees

In our approach, the IOE of each agent is modelled by using decision tree regression. The inputs of IOE are used as the feature set and the output is used as the dependent variable to train the decision tree regression model. In this section, we briefly discuss the rationales behind this design choice.

One very important consideration for us is the comparability of the regression model. To clarify, consider an advisor agent and an advisee agent with heterogeneous IOEs. The main goal of modelling their IOEs is to transform them into a common space to compare and derive possible correlations between them. Hence, black-box models such as neural networks are not much helpful for this purpose. Also, logistic regression and support vector machine (SVM) do not produce output models which can seamlessly be used to derive possible correlations. Since decision trees are flowchart-like hierarchical data structures, they can be easily used in an automatic mechanism to derive the aforementioned correlations, as described in Section II-A. Besides, decision trees are highly robust on small datasets which is the case of this paper since the IOE of each agent is individually modelled and the training set is the agent's own first-hand evidence space.

III. A Running Example

In this running example, we consider the scenario of Internet data plan sharing in a smart city. To better clarify, we will first describe the agents in the mentioned scenario, then explain Internet data plan sharing and elaborate on where trust is needed and why subjectivity can be an issue for the trust system in that scenario. Finally, we will explain in full details how our proposed mechanism can be applied to solve that issue.

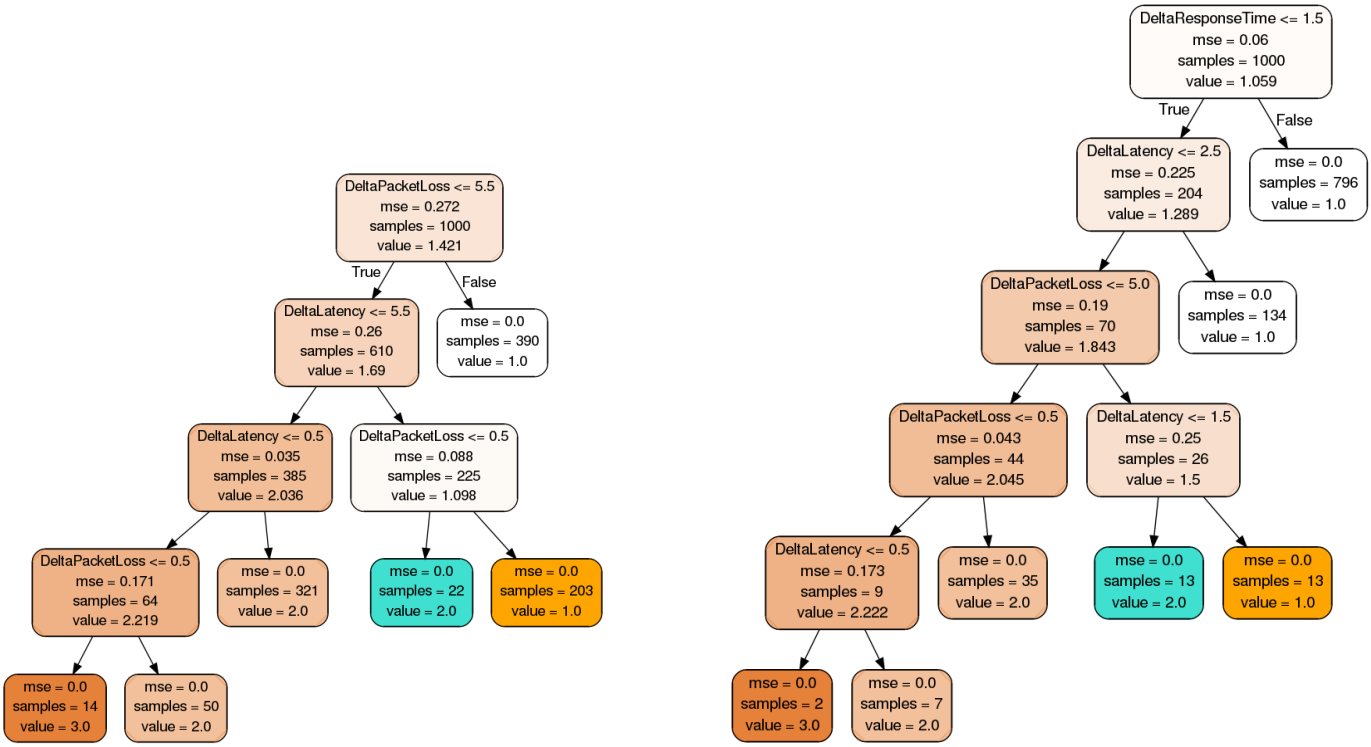


Fig. 2: (a) Decision tree regression for environmental sensors. (b) Decision tree regression for smart cars.

There are three types of agents in our smart city Internet sharing scenario :

- **Environmental Sensors:** These sensors monitor environment related variables (e.g. noise level, air pollution, etc.) and need to periodically report to the base station, which requires brief opportunistic Internet connectivity (i.e. few times a day, small batches of data transmission).
- **Smart Cars:** They need to periodically check for security updates which again requires brief opportunistic Internet connectivity. Furthermore, vehicular ad hoc networks (VANET) can significantly benefit from this type of connectivity since it would decrease the dependency on road side units (RSU).
- **Smart Phones:** With the prevalence of enabling cellular technologies (e.g. 3G, 4G, etc.), many phones are connected to the Internet and also most of them have the ability to act as a wifi hotspot.

Smart phones can then sell their spare data plan to other agents who require brief periodic Internet connectivity. In the rest of this example we will refer to smart phones as service-provider agents and refer to environmental sensors and smart cars as service-requester agents. One important challenge in realization of such applications is the feasibility of maintaining a sound and scalable trust and reputation management system for this highly heterogeneous multi-agent space. So the smart cars and environmental sensors need to maintain a trust system based on their previous Internet data purchases (first-hand evidence) from the service-provider agents (smart phones) and request advice from each other to enrich their second-hand evidence space. The challenge that any trust system would face in this example scenario is that the potentially different IOE of heterogeneous adviser agents may result in misleading advice which is indistinguishable from dishonest advice. To better clarify on this, consider three quality of service (QoS) metrics as defined below:

- **Response Time:** The time it takes for the service-provider agent to accept or reject a data purchase request.
- **Latency:** The delay between sending a data packet and receiving its delivery acknowledgement.
- **Packet Loss:** The total number of lost data packets in each 15KB of data transmission.

The service-provider agents advertise their QoS metric values. Since they are self-interested agents, they can lie, which justifies the necessity of trust systems being used in such scenarios. Meanwhile, since service-requester agents are heterogeneous, they may evaluate the trustworthiness of the service-provider agents differently. For example, smart cars have high degree of mobility, so they have a significantly narrow encounter window (the time they will be in the wireless range of a service-provider agent). As a consequence, they are more sensitive to response time and latency, which leads to a different precision and priority for those specific metrics in their IOE compared to that of environmental sensors which are static. However, the environmental sensors in our example

are not connected to power grid and operate on small solar panels. As a result, re-transmission due to packet loss is very costly for them while smart cars do not have this limitation, and consequently they are not as sensitive to packet loss. In our example, these differences are accordingly reflected in the IOE mechanisms of environmental sensors and smart cars as represented by Eqn. 3 and Eqn. 4:

$$IOE_E = 3 - \left\lceil 0.1 \left\lceil \frac{\Delta L}{5} \right\rceil + 0.9 \left\lceil \frac{\Delta P}{5}) \right\rceil \right\rceil \tag{3}$$

$$IOE_S = \begin{cases} 1 & \Delta L > 4 \\ 1 & \Delta R > 2 \\ 3 - \left\lceil 0.9 \lceil \frac{\Delta L}{2} \rceil + 0.1 \lceil \frac{\Delta P}{5}) \rceil \right\rceil & Otherwise \end{cases} \tag{4}$$

where $\Delta L, \Delta R, \Delta P \in [0, 10)$ are the deviation of advertised values from perceived values for latency, response time and packet loss QoS metrics, respectively (e.g. $\Delta L = 4$ means that the perceived latency deviates 4 units from the advertised latency). Also, the output range for both IOE mechanisms is $\{1, 2, 3\}$ (e.g. dishonest, fairly honest, very honest).

As explained in Section II, the IOE of each agent is modelled by using decision tree regression. The corresponding decision trees for environmental sensors and smart cars are depicted in Figure 2. Therefore, whenever an environmental sensor i offers an advice $x \in \tilde{D}_i$ to smart car i', where $\tilde{D}_i = \{1, 2, 3\}$, it also offers the decision tree T illustrated in Figure 2a. Having x and T, for each outcome $j \in \tilde{D}_{i'}$, where $\tilde{D}_{i'} = \{1, 2, 3\}$, the smart car computes the posterior probability that j might be the outcome observed by itself given that outcome x has been observed by the environmental sensor i. Following Algorithm 1, a complete example for this process with x=3 (very trustworthy according to advice) is illustrated in Eqn. 5-7.

$$\begin{aligned} &p(T'(3)|T(3)) : \\ &= p(\Delta L, \Delta P <= 0.5 \wedge \Delta R <= 1.5 \mid \Delta L, \Delta P <= 0.5) \\ &= \frac{p(\Delta L, \Delta P <= 0.5 \wedge \Delta R <= 1.5)}{p(\Delta L, \Delta P <= 0.5)} \\ &= \frac{|\Delta L, \Delta P <= 0.5 \wedge \Delta R <= 1.5|}{|\Delta L, \Delta P <= 0.5|} \end{aligned} \tag{5}$$

$$\begin{aligned} &p(T'(2)|T(3)) : \\ &= p((\Delta R, \Delta L <= 1.5 \wedge \Delta P > 5) \vee \\ &(\Delta R <= 1.5 \wedge \Delta L <= 2.5 \wedge 0.5 < \Delta P <= 5) \vee \\ &(\Delta R <= 1.5 \wedge \Delta P <= 0.5 \wedge 0.5 < \Delta L <= 2.5) | \\ &\Delta L, \Delta P <= 0.5) \\ &= 0 \end{aligned} \tag{6}$$

$$\begin{aligned} &p(T'(1)|T(3)) : \\ &= p((\Delta R > 1.5) \vee (\Delta R <= 1.5 \wedge \Delta L > 2.5) \vee \\ &(\Delta R <= 1.5 \wedge \Delta P > 5 \wedge 1.5 < \Delta L <= 2.5) | \\ &\Delta L, \Delta P <= 0.5) \\ &= p(\Delta R > 1.5 \mid \Delta L, \Delta P <= 0.5) \\ &= \frac{p(\Delta L, \Delta P <= 0.5 \wedge \Delta R > 1.5)}{p(\Delta L, \Delta P <= 0.5)} \\ &= \frac{|\Delta L, \Delta P <= 0.5 \wedge \Delta R > 1.5|}{|\Delta L, \Delta P <= 0.5|} \end{aligned} \tag{7}$$

To further clarify, $p(T'(3)|T(3))$ in Eqn. 5 gives the conditional probability of a leaf node with a value equal to 3 being observed on the decision tree T' of the smart car given the event that a leaf node with a value equal to 3 has been observed on the decision tree T of the environmental sensor. The event $T(3)$ is equivalent to $(\Delta L, \Delta P) <= 0.5$ which can be obtained by traversing the decision tree of the environmental sensor from the root to the leaf node(s) with a value equal to 3. Similarly, the event $T'(3)$ is equivalent to $(\Delta L, \Delta P <= 0.5 \wedge \Delta R <= 1.5)$ which can be obtained by traversing the decision tree of the smart car from the root to the leaf node(s) with a value equal to 3. Under the same principle, $p(T'(2)|T(3))$ and $p(T'(1)|T(3))$ are then obtained in Eqn. 6 and Eqn. 7, respectively.

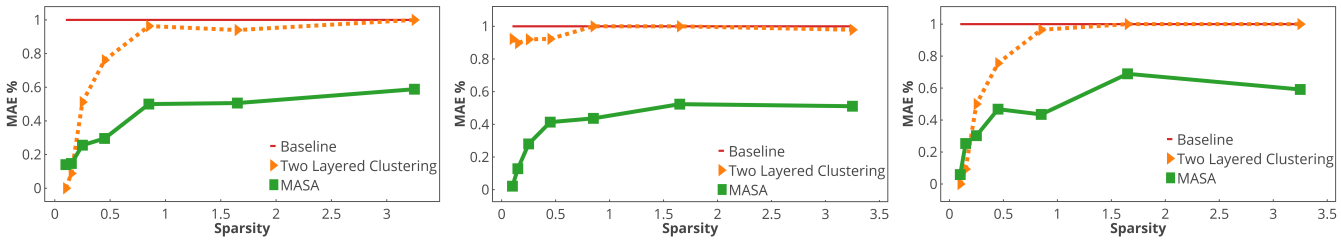
The final values for the probabilities in Eqn. 5-7 will be calculated with counting over a representative sample of the first-hand evidence space. For this example, we assume the values to be 30%, 0, and 70% respectively for $p(T'(3)|T(3))$, $p(T'(2)|T(3))$, and $p(T'(1)|T(3))$. These probabilities form a vector which represents the probability mass function of the subjectively aligned advice. Then variance-modulated entropy (Eqn. 2) is used on the calculated probability vector to weight the transformed advice as illustrated in Eqn. 8.

$$\begin{aligned} &A = [0.7, 0, 0.3] \\ &\lambda = (1 - H(A))^{\frac{\sigma^2(A)}{\sigma^2(U\{1,2,3\})}} \\ &\lambda = 0.679 \end{aligned} \tag{8}$$

The resulted $\lambda(A)$, then is passed to the underlying trust system as an evidence fusion weight and $\mu(A)$, the expected value of A, is passed as the subjectively aligned-second hand evidence.

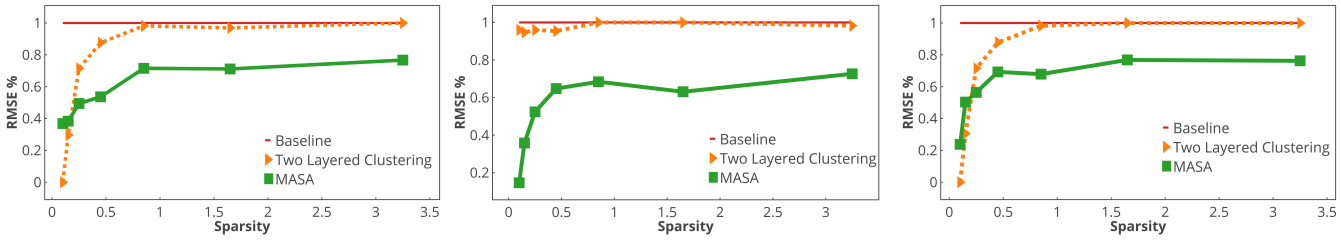
IV. Evaluation

We demonstrate how subjectivity can negatively impact the performance of the underlying trust system in IoT, and evaluate the effectiveness of MASA, by conducting two extensive simulations. First, we simulate the scenario of Internet data plan sharing in a smart city. Second, we simulate an IoT-based crowd-sensing application in the transportation domain. We also apply our approach on real data obtained from MovieLens dataset to further validate the efficacy of MASA and indicate that MASA can also be applied to other domains besides IoT.



(a) (b) (c)

Fig. 3: MAE for different sparsities where (a) 30% (b) 50% (c) 70% of the advisor agents are smart cars.



(a) (b) (c)

Fig. 4: RMSE for different sparsities where (a) 30% (b) 50% (c) 70% of the advisor agents are smart cars.

A. *Internet data plan sharing in smart cities*

In this section, we adopt the scenario of Internet data plan sharing in a smart city as explained in section III with details. We have compared our approach (MASA) with one previous approach [3] referred to as two layered clustering which addresses the subjectivity issue in trust management and a baseline which does not consider subjectivity at all and aggregates all the advice. We have calculated the *root mean square error (RMSE)* and *mean absolute error (MAE)* of the aforementioned three different approaches under different evidence sparsities. The ratio of total advisibles (smartphones) to total number of advice in the simulation is considered as a measure of the sparsity of second-hand evidence space as shown in Eqn. 9:

$$sparsity = \frac{\#Advisibles}{\#Advice} \tag{9}$$

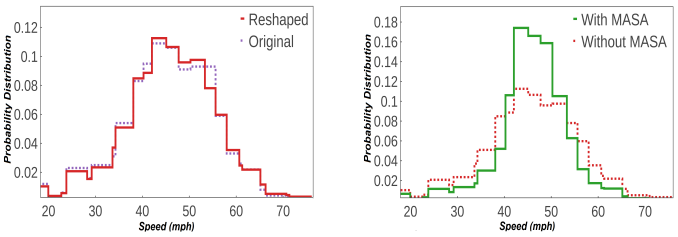
We have also considered three different situations in which respectively $30\%, 50\%$ and 70% of the advisor agents are smart cars and the rest are environmental sensors.

As we can see in Figure 3 and 4, with the sparsity of the second-hand evidence increasing, MASA outperforms the two layered clustering approach [3]. It is also notable that under high sparsity, two layered clustering loses its effectiveness and performs no better than the baseline while MASA converges to a fair effectiveness being approximately around $50 - 60\%$ of the baseline in terms of MAE ($60 - 70\%$ in terms of RMSE). Moreover, the effectiveness of the clustering approach is dependent on the accuracy of clustering. Hence, in cases where accurate clusters are not formed (Figure 3b and 4b), the approach can lose effectiveness while MASA does not suffer such restrictions, which makes it a perfect candidate for highly heterogeneous decentralized environments.

B. *IoT-based crowd-sensing application*

We adopt the scenario of the IoT-based crowd-sensing application in the transportation domain proposed in [8]. It monitors the average traffic speed of a major road (ground truth is $45mph$), by collecting GPS readings from crowd agents. We have two sets of crowd agents: drivers' car-borne GPS sensors dominantly as the contributing crowd and passengers' smart phone built-in GPS sensors dominantly as the advising crowd rating the accuracy of sensed data provided by the contributing crowd. These ratings will be utilised to reshape the probability distribution of the crowd-sensed data using the trust mechanism proposed in [8]. We have used the same simulation setup with the sole difference that each agent in the advising crowd votes *subjectively* on the accuracy of the data sensed by the contributing crowd, subjected to its sensor precision. The sensor precision of the advisors is considered as a log normal random variable with the mean equals to the sensor precision of the advisee agent and the skewness equals to 75% of the sensor precision of the advisee agent.

As depicted in Figure 5a, in the presence of a subjective advising crowd without MASA, the advising crowd is not significantly helping the advisee to better reshape the probability distribution of the crowd-sensed data towards the ground truth $45mph$. That is because advisors with different speed sensor precisions provide subjectively divergent feedbacks for the same crowd-sensed measurement. However, as depicted in Figure 5b, with incorporating MASA into the same system as a plugin to align the subjective feedbacks, the improvement is



(a) (b)

Fig. 5: (a) probability distribution of the original and the reshaped crowd-sensed data. (b) probability distribution of the reshaped crowd-sensed data with and without MASA.

significant, increasing the credibility of crowd-sensed data by almost 54% .

C. Experiment on Real Data Obtained from MovieLens

Here we apply MASA to the data that we obtained from MovieLens data set. We randomly select a movie x, and among the users who rated the movie we randomly pick one. We refer to that randomly selected user as *advisee*. Then, we try to predict advisee's rating on movie x based on the ratings that previous users (*advisors*) have submitted for movie x taking into account the decision trees of the advisors and the advisee. We repeat the procedure 1000 times. Some missing information from the MovieLens data set was obtained by crawling IMDB (e.g. movie language, movie duration, MPAA content symbol). The features used to train the decision trees in this experiment contain genres, language, duration, year, and the MPAA content symbol of the movie. As illustrated in Table I, MASA has also potential to be utilised in the reputation evaluation of non-autonomous agents despite not being the main focus of this paper.

TABLE I: MAE and RMSE of different approaches.

Methods	MAE	RMSE
Baseline	1.502	2.025
Two Layered Clustering	1.339	1.757
MASA	**1.215**	**1.693**

V. Discussion and Related Work

First and foremost, as illustrated in Figure 3 and Figure 4, MASA does not lose its efficacy when the first-hand evidence is sparse. This is of great importance since with the prevalence of IoT and growing number of devices, the first-hand evidence has become too sparse.

Furthermore, no assumptions are made in our simulations or the experiment about the underlying trust and reputation system. This highlights the fact that MASA can be incorporated into any of the existing trust or reputation systems, simply as a plugin. The significance of this independence becomes obvious as a consequence of the large heterogeneity in IoT devices. To further clarify, consider two agents with heterogeneous trust systems (e.g. one binary trust and the other non-binary trust). MASA will realize interoperability between these two agents.

Finally, each computation in MASA is performed either to model the IOE of an agent or to align a recently received advice. The computation required to obtain the IOE of each agent can be performed by the node which the agent is representing, since it only requires the first-hand evidence of that agent. Moreover, the computation required to align any received advice can also be performed by the advisee node, since it mainly requires advisee agent's IOE model, which is obtained from its first hand evidence and the IOE model of the adviser, which is received together with the advice. This enables all the computations of MASA to be performed in a completely decentralised manner which increases its scalability. Given the continuously growing number of devices, scalability is a crucial recruitment for any IoT related solution.

However, as indicated in Figure 3 and Figure 4, in the presence of extremely dense first-hand evidence, existing approaches such as [3] may slightly outperform MASA in terms of accuracy for some distributions of the subjective advisers (particularly, when the distribution is not even, e.g. 70% smart cars and 30% environmental sensors).

Another limitation of MASA is the reliance on interaction features, since these features together with the interaction outcome are used to train a regression model to represent the agent's IOE. Although the interaction features are never shared with other agents, and hence pose no privacy risks, they may not be simply available in some systems (e.g. when humans are asked to evaluate their interaction with an entity but it is not clear what their judgement is exactly based on). In practical trust and reputation systems this is mitigated by exposing human advisers to additional questions after they submit their rating (e.g. in Uber this is framed as "What can be improved?"). The decrease in performance as noted when comparing the results indicated by Table I and those of Figure 3 and Figure 4, highlights this limitation of MASA. Since the interaction features in the MovieLens dataset are not available, an educated guess has been made in our experiment to determine those features. Precisely, genre, language, duration, year, and the MPAA content symbol of the movie have been considered as the interaction features. Clearly, this guess may not be the complete set of the features which affected users' judgement. This explains the decrease in performance compared to when the interaction features are fully available.

There is little work on trust management for IoT [9]. The works [6] and [7] provided a trust-based service management for Social Internet of Things (SIoT) where IoT nodes can establish social relationships in favour of their human owners. The Idea of SIoT however was formerly introduced by [10] where the necessity of trust is highlighted for social IoT nodes which supposedly establish relationships and request/provide services autonomously. In [6], each node keeps a friendlist, a frequently visited location list and a device interaction list for calculating trust. However, in the presented model, nodes have to share this information with each other which may

raise privacy concerns. A later work [7] considered three trust properties: honesty, community-interest and cooperativeness as the key essence of the proposed trust calculation model, arguing that the final trust composition is application-specific since each IoT application can have different trust requirements with regards to these three trust properties. However, [11] took a different approach by providing two models: subjective and objective models. In the subjective model, each node calculates the trustworthiness of its friends using direct observations (first-hand evidence) and the indirect observations (second-hand evidence) from mutual friends. However, it leverages the assumption of similar subjectivity among friends which is highly open to debate (e.g. two friends can have fundamentally different points of view. Hence, friendships do not necessarily form on the basis of perspective similarities).

The issue of subjectivity in trust management of IoT systems is not well studied. However, there are a few works outside the IoT domain which try to address subjectivity issue while they have restrictive assumptions which do not fit IoT well. For instance, [2] assumed strong naive independence between the attributes that influence the subjectivity, which does not hold for IoT applications (e.g. knowing that a phone has a low resolution camera implies an old model and hence decreases the odds for it to have a near-field communication sensor). Clustering is used in [3] to group similar-thinking users together based on their provided ratings. However, it took a centralized approach assuming that the transaction history of all users is available at one entity which performs the clustering. Moreover it does not perform well when the first-hand evidence is sparse which makes it unfit for IoT applications.

To the best of our knowledge, we are the first to address subjectivity issue in trust and reputation management of IoT systems in a holistic manner.

VI. Conclusion and Future Work

Due to the high variance in IoT devices' sensor limitations, power and bandwidth constraints, privacy concerns, etc., IoT is featured with unprecedented heterogeneity which significantly aggravates the subjectivity issue in trust and reputation systems. To address this issue we proposed MASA, a multi-agent subjectivity alignment mechanism. Our evaluation results demonstrate the effectiveness of MASA and indicate that the efficacy of MASA is not limited to IoT. In our future work we aim to explore and address the context awareness and its influence on subjectivity.

References

[1] H. Yu, Z. Shen, C. Leung, C. Miao, and V. R. Lesser, "A survey of multi-agent trust management systems," *IEEE Access*, vol. 1, pp. 35–50, 2013.

[2] H. Fang, J. Zhang, M. ensoy, and N. M. Thalmann, "Sarc: subjectivity alignment for reputation computation," in *AAMAS*, 2012, pp. 1365–1366.

[3] H. Fang, J. Zhang, and N. Magnenat Thalmann, "Subjectivity grouping: learning from users' rating behavior," in *AAMAS*, 2014, pp. 1241–1248.

[4] F. M. Harper and J. A. Konstan, "The movielens datasets: History and context," *ACM Trans. Interact. Intell. Syst.*, vol. 5, no. 4, pp. 19:1–19:19, Dec. 2015. [Online]. Available: http://doi.acm.org/10.1145/2827872

[5] C. Strobl, J. Malley, and G. Tutz, "An introduction to recursive partitioning: Rationale, application, and characteristics of classification and regression trees, bagging, and random forests," *Psychological methods*, vol. 14, pp. 323–48, 12 2009.

[6] 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, pp. 684–696, 2016.

[7] 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, pp. 482–495, 2016.

[8] T. Luo and L. Zeynalvand, "Reshaping mobile crowd sensing using cross validation to improve data credibility," in *IEEE GLOBECOM*, 2017.

[9] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.

[10] L. Atzori, A. Iera, and G. Morabito, "Siot: Giving a social structure to the internet of things," *IEEE communications letters*, vol. 15, no. 11, pp. 1193–1195, 2011.

[11] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on knowledge and data engineering*, vol. 26, no. 5, pp. 1253–1266, 2014.