Evaluating Peer Behaviour in Distributed Participatory Sensing

RAMAPRASADA R. KALIDINDI[1], KVSVN RAJU[2], V. VALLI KUMARI[2], C.S. REDDY[2]
[1]Department of Computer Science and Engineering
S.R.K.R. Engineering College
Bhimavaram-534204
[2]Department of Computer Science and Systems Engineering
College of Engineering (A), Andhra University
Visakhapatnam-533003
INDIA
rrkalidindi@computer.org, kvsvn.raju@gmail.com, vallikumari@ieee.org, csatyanand@gmail.com

Abstract: - Recent advances in ubiquitous computing and availability of low cost sensors have led to the wide spread use of sensor networks in civilian applications. These networks along with multisensory personal devices generate lot of data in digital domain. Harnessing this data for urban sensing applications reduces the cost of implementation. This is possible when people share their data as a community service. However, people hesitate to participate because of trust deficit. Instilling trust among the participants will enhance people's participation and make a way for newer applications to share data among people. This paper describes a model for data sharing by computing confidence among networked peers. The social interactions in digital domain and reputation in community establish goodwill among peers. This goodwill and the trust on various control factors that influence a peer are used to evaluate its behaviour. However, trusting on peer's behaviour may involve risk otherwise there is an opportunity. More of opportunity than risk induces confidence on a peer. Finally, this confidence in peer decides whether to share data or not.

Key-Words: - Trust management, Privacy control, Risk, Behaviour aware computing, Participatory sensing, Urban sensing.

1 Introduction

Wide availability of low cost sensors and multisensory personal devices enable innovative services like community healthcare, public safety and city resource management [1, 2]. These sensors and personal devices generate high granular data from physical spaces. This data availability in virtual space creates a set of new applications in the form of opportunistic sensing and participatory sensing.

In opportunistic sensing, the application automatically determines usage of sensing device when its state matches application requirements. This approach needs resources to make a decision on when to use sensing device. Once accepted the users do not have any control over their data. Those people who are more concerned about their privacy may not be willing to allow the automatic data collection. Participatory sensing incorporates participant's decision to have control over their data [3]. People need privacy. This privacy is not solitude but control over their physical spaces. In virtual space, the control includes what data to share, which application request to accept and the extent of privacy preservation affecting data fidelity.

Revealing data collected by personal devices and sensors could have more number of risks on privacy of an individual than personal data (*viz.*, name and id). For example, location and health data reveal much about individual's interests and diseases leading to unwarranted problems. Without anonymization or control, people are less likely to share their personal data. Protecting privacy involves issues like identification of other person with whom data to be shared, amount of data and how long the data will be retained.

To protect privacy, data anonymization techniques are useful in applications like estimating the communicable disease spread (e.g., Google flu trends) and vehicular networks, etc. In applications like community healthcare anonymizing patients' data may not serve the purpose. Designing systems for these applications necessitates control and decision making at user's end. Control on with whom we are sharing data and what data we are sharing will induce confidence in users. In addition to data privacy, trusting the data source and trust on the people with whom data is shared are also important design aspects of these systems.

For example, consider the use case where citizens install their sensor networks in their residences in a gated community. As shown in Fig.1, sensors connect to cluster head in each residence. These cluster heads form a network connecting to Internet through a base station [4].

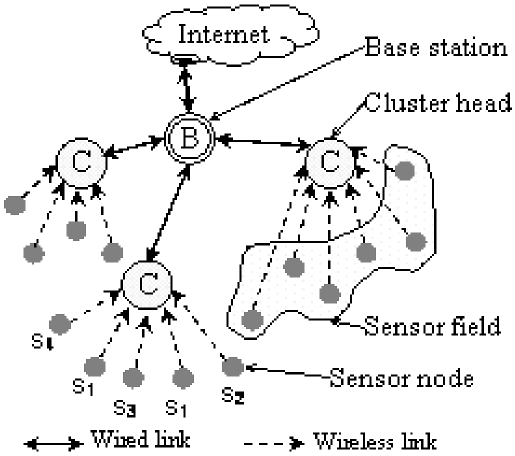

Fig.1 Distributed Sensor Networks [4]

This creates a distributed environment where each cluster head can communicate with its peer through base station or a remote entity through Internet. The residents can participate in city resource management, community healthcare and public surveillance etc, without installing extra hardware thereby reducing the cost in urban sensing applications. In urban sensing, the data sensed in-situ is more precise than remote sensing but it costs prohibitively high if the sensing area is very large. Participatory sensing reduces this cost. Proper usage of citizens' personal data and keeping the control over data with them instill confidence thereby increasing the participation.

This paper proposes a model to share data in a peer-to-peer network with confidence as a measure. The interactions between peers are assessed, positive or negative, by evaluating interaction property scores. These instructions influence opinion on a peer. This opinion and similar opinions obtained from other peers result in goodwill on a peer. External factors that influence the behaviour of the peer and goodwill are considered for the evaluation of behavioural trust. Since trusting on peer's behaviour may involve risk or may lead to an opportunity, these are estimated for each context. More of opportunity than risk results in confidence to share data.

In the section 2, related work was presented; section 3 describes proposed trust network model and calculation of trust from interactions between peers, section 4 describes the risk and opportunity involved in trusting a peer, section 5 finally describes building confidence in a peer to share data and section 6 concludes the paper and suggests possible future directions.

2 Related Work

Trust has been the focus of researchers in various domains starting from social sciences to e-commerce transactions [5]. It also plays major role in decentralized environment as in peer-to-peer networks and Internet. Recent attention is on trust as a measure to increase security and reliability of sensor networks. Trust is a derivation of the reputation of an entity [6]. Reputation is the opinion of one person about the other. Based on reputation a level of trust is conferred upon an entity. The reputation has been build overtime based on that entity's behaviour, and it may be positive or negative. Povey, in his paper described a mechanism for developing trust policy for authorization and web content using a risk management model [7]. It takes into consideration of beliefs about the parties being trusted, impersonal structures and systems involved.

Kalidindi *et al.* [4] described a model for participant driven privacy control in participatory sensing for better participation. In this model, users can exchange different types of data to different users depending on pre assigned authorization levels. Yao *et al.* uses access threshold for authorization by using points for different credentials to reveal private information [10]. Kalidindi *et al.* presented an opinion-based trust for privacy control in participatory sensing to share data [13].

Das and Teng [8] presented risk based view of trust and reviewed various concepts of trust. They attempted to integrate risk and trust by taking subjective trust, behavioural trust and trust antecedents as conceptualizations of trust. In their view, trust and risk are theoretical opposites. They argued that subjective trust and perceived risk assess the probabilities of the same event outcome. Josang and Presti [9] analysed the relationship between trust and risk in a transaction based decision-making process with risk information. They integrated trust and risk notions. Their model of trust considers the reliability trust as the probability estimate of transaction success and defined a measure that represents trusting decision, which they call decision trust. Ruizhong *et al.* presented a dynamic trust model based on perceived risk considering user's subjective perception factors [11]. Lund *et al.* presented evolution in risk assessment and trust management with different perspectives [12]. They presented a method to take trusting decisions by weighing opportunity and risk.

3 Trust Network Model

Let there be '*n*' nodes (N_1 - N_n) in a peer-to-peer network. Any node can be a trustor node and any one from the remaining can be trustee node [14]. In the trust network model shown in Fig.2, node N_i is the trustor node and N_j is the trustee node and the nodes can communicate with each other. The lines connecting different nodes indicate interactions between nodes.

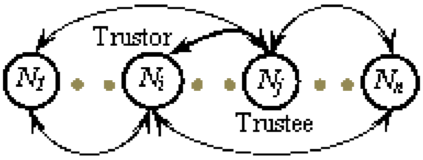

Fig.2 Trust network model

The two connected nodes can interact with each other. Each node maintains its opinion about other nodes and a node can request other nodes to give opinion about a node. We assume, Network is robust and free from failures and propagation delays are negligible. Since the nodes can willingly participate in the network we assume them to be honest, but this need not be correct always.

3.1 Interactions

In the trust network model shown in Fig.2, the communication takes place in the form of requests and responses. In the absence of request and responses, communication will not take place between nodes, where as in the remaining possibilities communication takes place.

An interaction can be defined as the communication between nodes in the form of request, response or both. The trustor requests and trustee responds, request is a part of an interaction from trustor where as response is the other part of that interaction from trustee. No interaction takes place in the absence of request and response. The trustor judges these interactions as positive and negative depending on the following criteria:

1) No response from trustee for the request made is a negative interaction.
2) Getting response from trustee for a request made (or without a request) is judged as positive or negative interaction depending on various properties like time taken to respond for a request; frequent exchange of data; reciprocity; relevance of data exchanged to the request made; etc., [13].

The status of the interaction, either positive or negative, is determined depending on various factors represented by interaction properties [11, 15]. Let t_{ij} be the total interactions between trustor N_i and trustee $N_{j.}$ and t_{ij}^p are positive and the remaining are negative interactions. $P = \{p_1, p_2, ..., p_m\}$ is the set of *m* properties for an interaction and I_k is the score for k^{th} property. $I \in [0,1]$ is the aggregated weighted score which determines whether an interaction is positive or not. Depending on the status of overall interactions, personal opinion (*ib.* §3.2) on the trustee is calculated. We consider the following five properties for an interaction.

3.1.1 Response time (p_1)

In many social situations when we ask for help from a neighbour, his prompt response for our request builds relationship. This is especially true in the case of emergencies. The response time is the elapsed time between request made by the requesting node and to the response from the responding node. This reflects the importance the responding node is giving to a request. Less response time gives more weightage for the interaction. Response time variations resemble inverse Gompertz curve, where decay is slowest at the start and end of a period and is represented as [16]:

$$I_1 = 1 - e^{-b_1 e^{-c_1 t_1}} \quad (1)$$

Where, I_1 is the response time score; b_1 and c_1 are constants and t_1 is the waiting time in hours between request and response. Fig.3 shows the forms of score variation for different b_1 values when c_1=0.5.

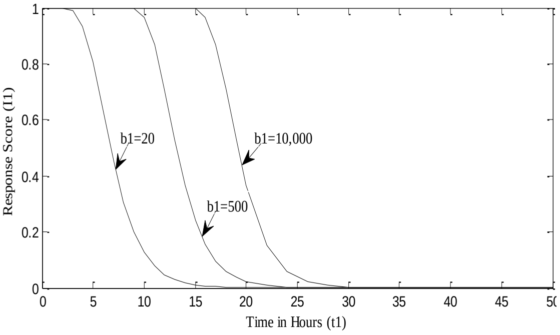

Fig.3. Response time score for different values of b_1 (20, 500, 10,000) when c_1=0.5

Since the node cannot wait infinitely for the response to a request. It will wait for certain amount of time to collect the responses from various nodes and inference is taken. The b_1 determines waiting time threshold and c_1 determines window in which the response is accepted with reduced weightage. The response time score I_1 is calculated by selecting b_1 to individual node's perspective on how much time it has to wait for the response. After selecting b_1 value, c_1 is selected as 0.5 to have sharp fall in response score such that there will not be any relevance for the response if it reaches after a threshold waiting time.

3.1.2 Time gap (p_2)

Relationship between nodes develops gradually with interactions. Beneficial acts of requesting node prompt reciprocal benefit from responding node, which result in frequent interactions. Continuous interactions result in better relationship where as discrete interactions show negligible relationship. The relation takes the form of a series of sequentially contingent acts; for example, our neighbour cares for our house while we are gone for a tour, we will bring gifts, he invites us to lunch when we return from tour, and so forth.

Continuous interactions can be identified by taking the inter interaction time gap. The time gap is the interval between present interaction and the immediate previous interaction of the requesting or responding node. Lesser time gap indicates extending relationship, higher time gap indicates discrete relationship. Indirectly this property gives higher weightage for the interaction from a node, which is maintaining continuous relationship. Time gap variations also resemble inverse Gompertz curve and is given as [16]:

$$I_2 = 1 - e^{-b_2 e^{-c_2 t_2}} \qquad (2)$$

Where, I_2 is the time gap score; b_2 and c_2 are constants and t_2 is the time in months. Fig.4 shows the forms of score variation for different c_2 values when b_2=10.

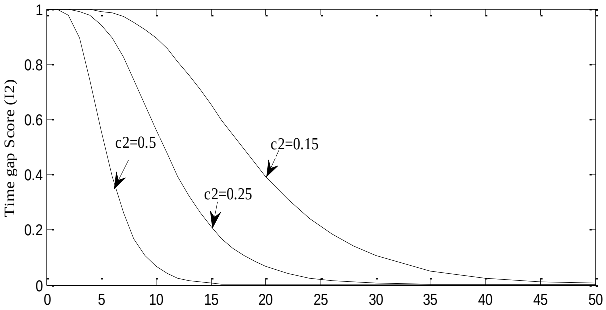

Fig.4. Time gap score for different values of c_2 (0.5, 0.25, 0.15) when b_2*=10*

The b_2 determines maximum time gap threshold between interactions in continuous interactions; c_2 determines window in which present interaction is related to immediate previous interaction for determination of continuous interactions, which will have higher weightage.

The time gap score I_2 is calculated by selecting c_2 value to individual node's perspective on whether the interaction is occasional or frequent and b_2 value is taken as 10 because we need not wait to determine the interaction as a continuous one or not. As the inter interaction time gap increases the relationship ceases to be a continuous relationship.

3.1.3 Familiarity (p_3)

In society, long lasting relationships weigh more than nascent relationships. The amount of exposure people have to each other influences these relationships. Over time, as the interactions between requesting and responding nodes increase the familiarity increases. This increase resembles Gompertz curve, where growth is slowest at the start and end of a period [16]. The score for this property is given as:

$$I_3 = e^{-b_3 e^{-c_3 t_3}} \qquad (3)$$

Where, I_3 is the familiarity score; b_3 and c_3 are constants and t_3 is the time in years. The curve forms for various c_3 values and b_3=10 are shown in Fig.5.

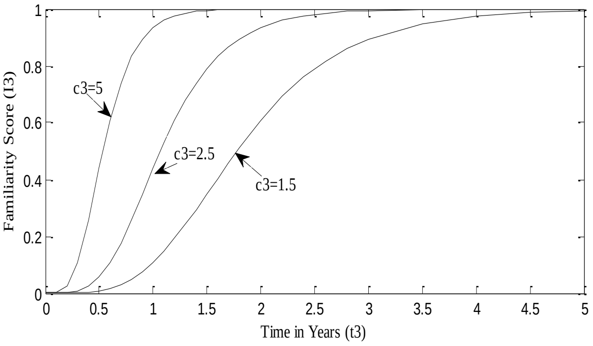

Fig.5. Familiarity score for different values of c_3. (5, 2.5, 1.5) when b_3=10

The selection of b_3 and c_3 represents the node's perspective about the familiarity, where low c_3 value takes more time and high c_3 value takes less time to get full familiarity. The b_3 value is taken as 10. As time passes by familiarity increases, thereby we need not wait for starting familiarization.

3.1.4 Reciprocity (p_4)

In our daily life, reciprocal acts of benefit, viz. offering help, advice, approval etc., form social exchange [17]. This reciprocity is an indicator of stability in social relations [18]. In building relationships, people observe how far the other person is reciprocating for their gestures. Reciprocal exchanges build relationships and lack of reciprocity ruins relationships.

The reciprocity is considered as the extent of contextual or personal data that responding node is sharing with requesting node. Otherwise, it can be authorization level given by responding node to requesting node to access its own data. The nodes divide their privacy levels according to their convenience, *viz.* 3, 5, 10 levels or as percentage. The highest level is free access or zero privacy and lowest level is no access or full privacy. One of these levels is allowed as a reciprocal gesture by the responding node to the requesting node. Since the requesting node can access data, we assume that it knows the number of levels, max., min. and its privilege levels. To get normalized score for different nodes the reciprocity score I_4 is given as:

$$I_4 = \frac{r - r_{\min}}{r_{\max} - r_{\min}} \qquad (4)$$

Where, r is the privilege/authorization level given by the responding node to the requesting node; $r_{\max}$ is the maximum level representing free access at the responding node; $r_{\min}$ is the minimum level representing no access at the responding node and $r_{\min} \le r \le r_{\max} \in [0,1]$.

3.1.5 Relevance (p5)

When we approach for help to our neighbors, if the response from our neighbors is not to our expectations it will disappoint us. Some may give irrelevant gestures, which may not be useful to us. Relevance property reflects the relevance of the response for the request made by requesting node, which is a subjective judgement.

In reality, most of the parameters in our social interactions are subjective in nature. To determine the score for subjective type of properties; a grading level F_k for each property p_k is assigned as: $F_k = G_k(p_k)$. Where G_k is the grading function of property p_k, which converts property value into the corresponding grading level. Score intervals I_k of each property are calculated as: $I_k = S_k(F_k)$. Where S_k is the score function that maps grading level.

To obtain relevance score I_5 the grading levels are mapped to five score intervals [0, 0.25, 0.5, 0.75, 1]. Table 1 gives scores for corresponding grading levels.

For an interaction, not all interaction properties are equally important; some properties (viz. reciprocity and familiarity) have more influence than others do. So user can give relative importance using weight w_k^p to each property, such that $w_k^p \in [0,1]$, $\sum_{k=1}^{m} w_k^p = 1$.

Table 1: Grading levels and Scores for Relevance

Grading levels	**Score**
Not at all relevant	*0.00*
May not be relevant	*0.25*
Can't say	*0.50*
Relevant to some extent	*0.75*
Fully relevant	*1.00*

Table 2 gives weight for each interaction property. A node can set weights according to its perception about an interaction.

Table 2: Weights of interaction properties

Interaction Property (pk)	w_k^p
Response time (p1)	0.2
Time gap (p2)	0.1
Familiarity (p3)	0.3
Reciprocity (p4)	0.3
Relevance (p5)	0.1

The sum of weighted scores I is given as:

$$I = \sum_{k=1}^{m} \left(w_k^p \times I_k \right) \qquad (5)$$

The interaction is positive if $I \ge (1 - T_b)$, where $T_b \in [0,1]$ is the behavioural trust (probability expectation of benign trustee behaviour, *ib.* §3.3.4) on a node. Initially T_b is not equal to zero but it will have a minimum value (because of to trust due to control, *ib.* §3.3.3) thereby having a maximum threshold which is less than one. As the trust increases, this threshold decreases as it happens in reality when we deal with friends and new acquaintance. When the behavioural trust on a node is high, the possibility of interaction being positive is also high. These interactions are necessary to form an opinion on other nodes.

3.2 Opinions

In our social interactions, our relationship will vary from stranger through the acquaintance. People trust acquainted persons depending on the interactions with them and stranger too is trusted to some extent. People will form opinion either positive or negative based on interactions they have with others. As per the definition, the *opinion* is “a view or judgment about a particular thing, which is not necessarily based on fact or knowledge” [19]. When this opinion is based on personal interactions, it is called as *personal opinion*. In the proposed model, personal opinion about a node is calculated depending on the status of the node's overall interactions with that node. Likewise, for every node in the network personal opinion is calculated and is stored in an opinion table (*ib.* Table 3).

In the absence of interactions or in the case of doubt, people consider the opinion of the acquainted persons. These opinions will have weightage depending on the trust that a person is having on the acquainted person. Mostly in this type of situations, the opinions of trusted persons will influence the decision making process. The collective opinion from such persons is *community opinion*. The opinion may be positive or negative. In the trust network model in Fig.2, the weighted personal opinions from each node about a node will be the basis for the *community opinion*. Here we consider both personal and community opinions for identifying the trust on the trustee.

3.2.1 Personal opinion

Personal opinion is the value given by a node depending upon the responses it is having from responding node. These responses are either positive or negative. The total interactions have both positive and negative interactions. Effective interactions are the difference between positive and negative interactions. The node N_i's *personal opinion,* Op_{ij}^{p} on N_j is the ratio of effective interactions to total interactions and $Op_{ij}^{p} \in [-1,1]$.

$$Op_{ij}^{p} = \frac{2\,t_{ij}^{p}}{t_{ij}} - 1 \qquad (6)$$

After determining whether the interaction is positive or negative using equation (5) the personal opinion is calculated using equation (6). If $Op_{ij}^{p} < 0$, N_i is having negative opinion on N_j, for $Op_{ij}^{p} > 0$ N_i is having positive opinion on N_j. For $Op_{ij}^{p} = 0$, N_i is not having any opinion. Each node assigns a weight to a node depending on its opinion about that node. The assigned weight $w_{ij}^{n} \in [0,1]$ to a node N_j, at N_i is equal to the value of the personal opinion if positive interactions are more than half of the total interactions and zero for other values.

$$w_{ij}^{n} = \begin{cases} Op_{ij}^{p} & \text{if } t_{ij}^{p} > \dfrac{t_{ij}}{2} \\ 0 & \text{Otherwise} \end{cases} \qquad (7)$$

Each node will maintain an opinion table, as in Table 3, which contains its opinion on other nodes, their assigned weight, positive and total number of interactions with those nodes in the network. For every request made by the node, it updates the total number of interactions. The node will wait for response for a prescribed time and sends another request for another interaction.

Table 3: Opinion Table at Node ***N_i***

Node	**Opinion**	**Assigned weight**	**Interactions**	
			Positive	**Total**
N_1	Op_{i1}^{p}	w_{i1}^{n}	t_{i1}^{p}	t_{i1}
.	.	.	.	.
N_j	Op_{ij}^{p}	w_{ij}^{n}	t_{ij}^{p}	t_{ij}
.	.	.	.	.
N_n	Op_{in}^{p}	w_{in}^{n}	t_{in}^{p}	t_{in}

Fig.6 shows the procedure to update opinion and node's weightage with every interaction by calculating these values using equations (6) and (7) respectively.

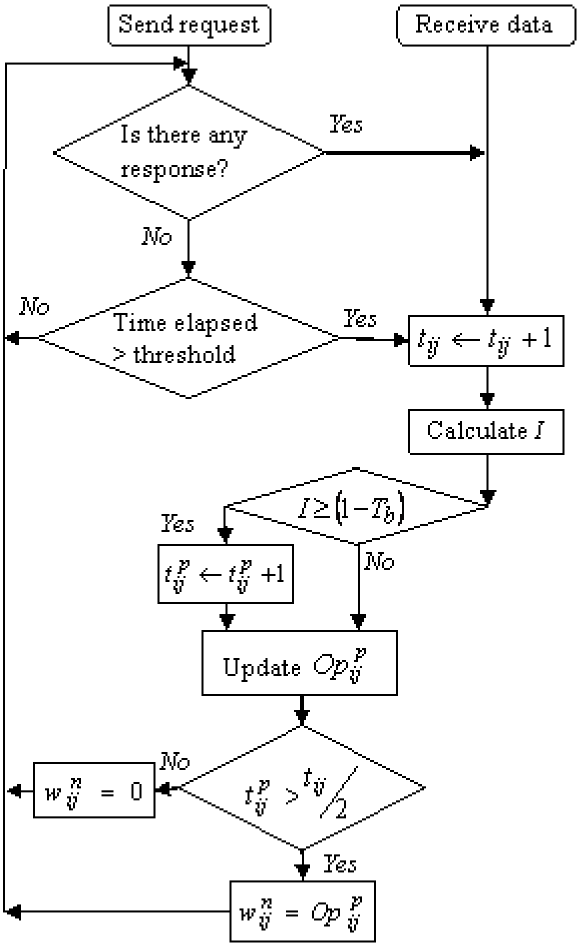

Fig.6. Updating opinion table (*ib.* Table 4)

3.2.2 Community opinion

Community opinion is the opinion collected from other nodes in the network. When a node N_i wants to calculate the opinion on node, N_j it sends a request to all other nodes. These nodes will respond to this request by sending the opinion on N_j, which is available in their respective opinion tables. A node that is having more interactions with target node can give better opinion about that node. The received opinion will have importance depending on responding nodes' weightage. Preference is given to the opinion collected from nodes whose weightage is more.

Let there be two opinion clusters OC_1 and OC_2. The first cluster OC_1 represents set of n_1 nodes whose weightage $w_{ix}^{n} \ge 0.5$ and OC_2 represents set of n_2 nodes whose weightage $w_{ix}^{n} < 0.5$.

The average opinion of the cluster OC_1 is given as:

$$Op_{c1} = \frac{\sum_{x=1}^{n_1}\left(w_{ix}^{n} \times Op_{xj}^{p}\right)}{n_1} \quad \text{for } w_{ix}^{n} \ge 0.5 \tag{8}$$

Where Op_{xj}^{p} is the opinion given by node N_x to node N_i;, w_{ix}^{n} is the weightage of the node N_x at the node N_i. ; and n_1 is the number of nodes giving opinion whose weightage $w_{ix}^{n} \ge 0.5$. If n_2 is the number of nodes giving opinion whose weightage $w_{ix}^{n} < 0.5$ and the average opinion of the cluster OC_2 is given as:

$$Op_{c2} = \frac{\sum_{x=1}^{n_2}\left(w_{ix}^{n} \times Op_{xj}^{p}\right)}{n_2} \quad \text{for } w_{ix}^{n} < 0.5 \tag{9}$$

The clustering algorithm [20] as shown in Fig.7, is applied on the two opinion clusters.

Setup: Each node in the trust network model maintains an opinion table, which consists of opinion about other nodes, assigned weights to each node and number of interactions with other nodes. After forming the opinion clusters, the returned value Op_{c1} is community opinion about node N_j at node N_i.

Input: Opinions from responding nodes Op_{xj}^{p} and their weights w_{ix}^{n}.

Output: Resultant average opinion Op_{c1} of the opinion cluster OC_1

Steps:

```
1: Initialize
    (i) Opinion clusters $OC_1$ and $OC_2$ for nodes whose $w_{ix}^{n} \ge 0.5$ and $w_{ix}^{n} < 0.5$ and $n_1$ and $n_2$ as number of nodes in each of these clusters respectively.
    (ii) $Op_{c1}$ and $Op_{c2}$ as cluster centers for opinion clusters $OC_1$ and $OC_2$ respectively and $n$ as the total number of nodes in two clusters.
until there are no changes in mean of $OC_1$
    for all nodes $(1 \le x \le n)$
        2: Calculate $d_1 = \left\| \left(w_{ix}^{n} \times Op_{xj}^{p}\right) - Op_{c1} \right\|$,
           $d_2 = \left\| \left(w_{ix}^{n} \times Op_{xj}^{p}\right) - Op_{c2} \right\|$ for node $N_x$
        3: If $d_1 < d_2$ then node $N_x \in OC_1$; else
           $N_x \in OC_2$ modify $n_1$ and $n_2$.
    end for
    4: Calculate $newOp_{c1} = \frac{\sum_{x=1}^{n_1}\left(w_{ix}^{n} \times Op_{xj}^{p}\right)}{n_1}$ for all nodes $N_x \in OC_1$ and
       $newOp_{c2} = \frac{\sum_{x=1}^{n2}\left(w_{ix}^{n} \times Op_{xj}^{p}\right)}{n_2}$ for all nodes $N_x \in OC_2$.
    5: Assign $Th = \left|Op_{c1} - newOp_{c1}\right|$,
       $Op_{c1} = newOp_{c1}$ and $Op_{c2} = newOp_{c2}$
end until $Th < 0.001$
Step 6: Return $Op_{c1}$
```

Fig.7. Finding opinion clusters

The final opinion cluster center Op_{c1} represents convergence of most of the opinions and is taken as the community opinion Op_{ij}^{c}. These personal and community opinions bestow trust on trustee node.

3.3 Trust

Humans are social by nature and their relationships in society are based on traditional face-to-face or human-to-human interactions. Trust is an essential part of these interactions. As we move to information society and virtual world, agents and policies resembling that of humans influence these interactions [21, 22]. This necessitates trust management between computer agents. Trust is one of the more frequently used concepts in social sciences, psychology, philosophy, sociology, organization theory, and economics and recently in computer science. It is well known and yet less understood concept. The literature has given variety of meanings to trust with definitions covering notions as diverse as positive belief, personal trait, action, situational feature and social structure [8, 23].

Trust often used to refer the personality characteristics that make a person *trusting* and *trustworthy.* While *trustor* refers to the trusting party, *trustee* is the party being trusted. More importantly, it is a directional relationship between two parties, i.e. when *A* trusts *B*, that does not mean that *B* is also trusting *A*. When trustor is trusting trustee, it may be based upon innocence, impulsivity, conformity, virtue, faith, masochism, despair or confidence [24]. In this paper, the trusting choice considered is based upon confidence, i.e. upon trustor's assumption that the outcome he desires than outcome he fears will occur. When a trusting choice is made by a person *A* to share data with *B*,

i) *A* is aware that his choice could lead to misuse or productive use of data.

ii) *A* realizes that the consequences of his choice are depend upon confidence in *B*.

iii) *A* would expect to suffer much more if his trust in *B* is violated than he would gain if his trust is fulfilled.

The model described in this paper is from the perspective of the trustor. Here trust is not an objective property of trustor but subjective degree of belief about the trustee. When trustor trusts trustee, it means that the probability that trustee will perform an action that is beneficial or at least not detrimental to trustor. It is better for trustor to consider engaging in some form of cooperation with trustee. Correspondingly, when trustee is untrustworthy it means that the probability of performing beneficial action to the trustor is low enough to refrain from engaging in cooperation [25].

3.3.1 Dimensions of trust

Theorists have proposed that trust is a multidimensional concept, so it is necessary to differentiate various types of trust. Nooteboom suggests: (i) trust may concern a trustee's *ability* to perform as competence trust or (ii) his *intentions* to do so as goodwill trust [26]. Since goodwill and competence represent two independent sources of trust, they contribute to trust in separate ways. A banker may be regarded as highly reliable and trustworthy, but may not be competent enough to give higher returns. On the contrary, a stockbroker may be highly competent to give higher returns but one may have concern about his goodwill, given his intention to make as much commission as possible.

Josang *et al.* made a distinction between context independent and context dependent trusts calling them as reliability and decision trusts respectively [27]. The reliability trust gives an indication of general goodwill about the trustee. However, competence trust and decision trust differ. The competence trust gives an idea about the general competence of trustee to perform an event and decision trust gives an idea of trustee's competence to perform at that particular instant.

In summary, trust has two distinct dimensions of goodwill and competence, *i.e.*, when a trustee is having both goodwill and competence one can rely on him. The competence trust is dependent on capabilities of the trustee. In this paper, we assume that trustee's capabilities are good. Since the intention is to establish relationship between entities, here we consider the assessment of goodwill trust.

3.3.2 Goodwill trust

People constantly interact with others to form social communities. Social activities such as making new friends, helping others invite goodwill among the other members of the society. These social interactions build trust among the people. The building of trust on other person mainly depends on personal interactions with that person. However, in the absence of these interactions people depend on the reputation of that person in the society. That is, the goodwill on a person is the combination of our own observations and other's opinion about that person. When personal observations are more, then the importance of other's opinion decreases. The switchover from others opinion to personal opinion resembles Gompertz function.

Let w_i^o be the personal opinion weight at node N_i and 't_{ij}' is the number of interactions with node N_j and *u*, *v* represent constants. These constants determine how a person depend on his/her personal opinion with relative to others opinion. These depend on the attitude of the person and can be preset.

$$w_i^o = e^{-ue^{-vt_{ij}}} \tag{10}$$

The trust derived from the personal and community opinion on a node is the goodwill trust. The goodwill trust, T_g is obtained as:

$$T_g = w_i^o \times Op_{ij}^p + \left(1 - w_i^o\right) \times Op_{ij}^c \tag{11}$$

Initially when there are no interactions, the community opinion will have maximum weightage and as interactions increase, the personal opinion gains its importance. The Fig.8 shows two sets of plots for weightage variation for personal and community opinion.

The selection of constants in equation (10) depends on individual's personality and context. For example, in the first set where *u*=10 and *v*=0.4, one makes very fast switch over from community to personal opinion. A person will choose this one when he is capable of making decisions on his own and the application needs resources that are more personal. In the second set where *u*=5 and *v*=0.1, the transition is very slow and is suitable for applications such as community participation. It is suitable to persons who have a tendency to depend on others for making a decision. The goodwill trust obtained from opinions is considered for estimating the behaviour along with trust due to various control factors.

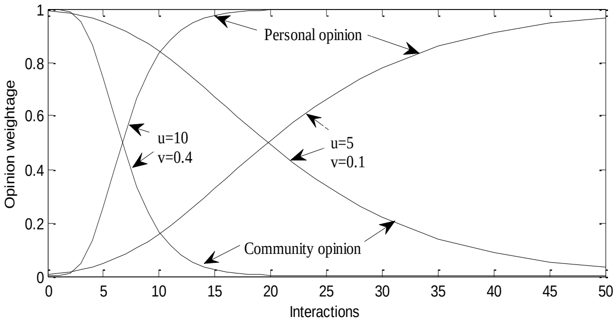

Fig.8. Opinion weightage *vs.* Number of interactions

3.3.3 Trust due to control

In society, many factors influence people to be trustworthy. Some of these factors are laws that compel people to follow common rules; binding agreements to follow; honesty and integrity that gives a person orderliness in daily life; social norms that establish common culture and values, etc. These control factors that influence the trustworthy behaviour of trustee will also contribute to the trust on the trustee [28, 29, 30]. The goodwill trust obtained by opinions will add up to this trust to form behavioural trust.

Let *C* be the set of *q* control factors $C = \{c_1, c_2, ..., c_q\}$ that influence the trustworthy behaviour of a node and Cf_{ip}^{p} is the node N_i's confidence in these control factors. The relative importance of these control factors is given by node N_i as control weight w_{ip}^{c} such that $\sum_{p=1}^{q} w_{ip}^{c} = 1$. For example, the user may consider control factors and his confidence on these factors and their relative weights of control factors as shown in Table 4.

Table 4: Control factors

Control factors (c_q)	Cf_{ip}^{p}	w_{ip}^{c}
Legal (c_1)	0.8	0.25
Agreement based (c_2)	0.9	0.30
Integrity (c_3)	1.0	0.30
Social (c_4)	0.5	0.15

Let $T_c \in [0,1]$ be the node N_i's trust on node N_j due to control factors and is given as:

$$T_c = \sum_{\mathrm{p}=1}^{\mathrm{q}} \left(w_{ip}^{c} \times Cf_{ip}^{p} \right) \qquad (12)$$

3.3.4 Behavioural trust

Goodwill trust is trustee's reputation among its peers and control influences trustee's behaviour due to the knowledge of punishment/incentive structure. Behavioural trust expects benign behaviour from trustee, which is the combination of both goodwill trust and trust due to control. It is the trust on someone's behaviour and allows the trustee to perform certain tasks, furnishing critical information to the trustee, placing the resources at the trustee's disposal, and so on [8: page 103].

Let $T_b \in [0,1]$ is the node N_i's trust on node N_j's behaviour and after normalization it is given as:

$$T_b = \frac{T_g + T_c + 1}{3} \qquad (13)$$

If the expectation of the behaviour is higher than the factual, there is a risk of disappointment and when it is lower, there will be a loss of opportunity.

4 Risk and Opportunity

In an environment of uncertainty, an event creates an opportunity to gain and a risk of loss. In this type of situations people make decisions using tools like trust and risk. As Das and Teng points out, risk is mirror image of trust [8]. A risky situation creates the need for trust. Both trust and risk represent the assessment of outcome probabilities of the same event from two distinctly different perspectives of hope and concern. Alternatively, trust is the probability of getting desired outcome, whereas risk is the probability of getting feared outcome. Along with these, there is an uncertainty, which refers to a condition of unsure outcomes.

Risk becomes salient once probabilities represent subjective trust. This is because the perceived risk is also the subjective estimation of probabilities. Consider the definition of trust by Josang *et al.* and Gambetta [25, 27], trust is the subjective probability by which trustor expects trustee to perform a given action on which trustor's welfare depends. By definition, trust is a belief the trustor holds about the trustee with respect to a particular action as a probability ranging from 0 (completely distrust) to 1 (completely trust). If the trustee performs as expected, it might have a positive effect on the trustor's welfare; otherwise, it might have a negative effect. The positive outcome corresponds to opportunity to gain in financial transactions or getting cooperation in the society and negative outcome correspond to risk of financial loss or loss of privacy in participatory networks [31].

Issues of trust arise when deception and betrayal are possible. The trustor knows that loss will occur due to this betrayal and in the absence of this deception; there is a chance of gain. That is, in a trust-based transaction, the trustor might be willing to accept the risk considering the opportunities involved or he might be willing to take the opportunity considering the risks involved.

Assume that the trustor has a trust level T_b in the trustee performing an action with gain g for the trustor and that deception has a loss l. The trustor must weigh the perceived opportunity $O(g,T_b)$ and perceived risk $R(l,1-T_b)$ against each other when deciding whether to engage in the trust based interaction [12, 31]. For example, consider an investment decision to get higher returns through a bank or a stockbroker. If a person wants to invest 1000 rupees in a bank for 10% interest and the trust on bank is 0.95, then he may get an interest of 100 rupees or he may lose entire invested amount.

$\textit{Opportunity value} = 100 \times 0.95 = 95$

$\textit{Risk value} = 1000 \times 0.05 = 50$

Since the opportunity value is greater than risk value, the person may consider depositing money in the bank. Similarly, if this amount is to be invested in shares through a stockbroker who promises to give 80% return and the trust in stockbroker is 0.5, then

$\textit{Opportunity value} = 800 \times 0.5 = 400$

$\textit{Risk value} = 1000 \times 0.5 = 500$

Even though the person expects 80% return, the risk value is greater than opportunity value. Therefore, the person may not opt for investing the money in shares. However if he expects a return of more than 100% he may invest in shares, because opportunity value will be greater than risk value.

Since opportunity and risk are involved, we assume that numerical data is available from the transaction context to compute opportunity level and risk level. In social situations, these values may be hard to determine practically, since many factors of the transaction need to be taken into consideration, and financial modeling as described in the above example may not be suited to all transaction contexts.

If the perceived risk value is higher than the perceived opportunity value for a particular node, data is withheld for sharing with that node. If it is otherwise, the node considers sharing data depending upon the confidence level on that node.

5 Confidence

Confidence is a belief that trustor can have faith in trustee. That is, trustor expects something to happen with certainty, and does not consider the possibility of anything going wrong. Confidence expects trustworthy behaviour from trustee; however, dependence on behaviour of the trustee may involve certain risk. Low risk in the perception of trustor instils more confidence in trustee [32, 33]. Fig.9 shows block diagram for obtaining trustor's confidence on trustee.

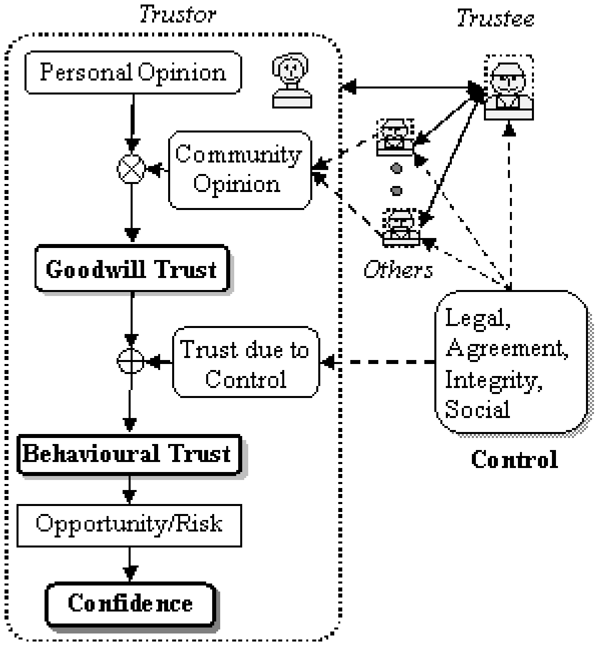

Fig.9 Confidence model

The goodwill trust is formed from the personal opinion and community opinion collected from other nodes. This goodwill trust and the trust on the control parameters like law, agreement, human integrity and social customs will form behavioural trust on the trustee. Expectations on one's behaviour involve certain risks and non-cooperation due to the fear of risk may lead to loosing the opportunity. More of the opportunity induces confidence so that trustor can go for sharing data with trustee.

6 Conclusions

Pooling up of citizen owned sensors' data to have applications for the common good of the society like city resource management, environmental monitoring, traffic monitoring etc, greatly reduce the cost of establishing standalone applications. The citizens can get peer help in case of emergencies by sharing data with neighbours;

however, risk is involved when this data goes to wrong persons. To reduce the risk, there is a need for identifying trusted parties in digital environment [21].

Most of the participatory sensing applications involve a centralized trusted party collecting data from the participants [34]. If this data is to be distributed among others, the centralized entity identifies trusted parties and gives them access control by authentication. When personal data is involved, access is given after anonymization. In these solutions, the participating entity is not having any trust on the receiving entity. People hesitate to share personal data to unknown persons through centralized entity thereby limiting people's participation in these applications.

Privacy control in the hands of participants encourages participation [4]. In this work, the participant directly identifies the trusted parties on its own. It considers the interactions in digital environment to establish trust. These interactions are useful in having an opinion on the peer and consider its reputation among peers to form goodwill. Trust established through this goodwill and the trust due to control factors that influence the peer's behaviour give an idea of how the peer behaves. Risk involved in depending on this behaviour is also considered to have confidence on the peer to share data.

Interacting with malicious intentions to increase goodwill trust and thereby deceiving; collusion between peers to give good opinion about a peer, are the areas for further study to have robust trust management in participatory sensing.

References:

[1] Shilton, K., Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection, *Communications of the ACM*, Vol. 52, No.11, 2009, pp. 48-53.

[2] Lane, N.D., Miluzzo, E., Lu, H., Peebles, D., Choudhury, T. and Campbell, A.T., A survey of mobile phone sensing, *IEEE Communications Magazine*, Vol. 48, No.9, 2010, pp. 140-151.

[3] Zhang, Guo, B. Li, B. and Yu, Z., Extracting social and community intelligence from digital footprints: An emerging research area, *Proceedings of the 7th International Conference on Ubiquitous intelligence and computing*, Springer, 2010, 15 pages.

[4] Kalidindi, R.R., Raju, KVSVN., Vallikumari, V. and Reddy, C.S., User controlled privacy in participatory sensing, *Proceedings of the International Conference on Advances in Computer Science*, 2010, pp.72-77. DOI: 02.ACS.2010.01.187

[5] Momani, M. and Challa, S., Survey of trust models in different network domains, *International Journal of Ad hoc, Sensor & Ubiquitious Computing*, Vol.1. No.3, 2010, pp.1-19.

[6] Ruohomaa, S., Kutvonen, L., and Koutrouli, L., Reputation management survey, *Proceedings of the 2nd IEEE International Conference on Availability, Reliability and Security (ARES'07),* 2007, 9 pages.

[7] Povey, Developing electronic trust policies using a risk management model, *Proceedings of the CQRE (Secure)'99*, LNCS 1740, Springer, 1999, pp. 1-16.

[8] Das T.K. and Teng, B.S., The risk based view of trust: A conceptual framework. *J. of Business and Psychology*, Vol.19, No.1, 2004, pp.85-116.

[9] Jøsang, A. and Presti, S.L., Analysing the relationship between risk and trust, *Proceedings of the iTrust 2004*, LNCS 2995, Springer, 2004, pp. 135-145.

[10] Yao, D., Frikken, K.B., Atallah, M.J. and Tamassia, R., Point based trust: Define how much privacy is worth. *Proceedings of ICICS 2006*, LNCS 4307, Springer, 2006, 20 pages.

[11] Ruizhong, Xiaoxue, M. and Zixian, W., Dynamic trust model based on perceived risk, *Proceedingsof the IEEE International Conference on E-Business and E-Government*, 2010, pp.2037-2040.

[12] Lund, M.S., Solhaug, B. and Stolen, K., Evolution in relation to risk and trust management, *IEEE Computer*, Vol., 43, No.5, 2010, pp.49-55.

[13] Kalidindi, R.R., Raju, KVSVN., Vallikumari, V. and Reddy, C.S., Trust based participant driven privacy control in participatory sensing, *International Journal of. Ad hoc, Sensor & Ubiquitous Computing*, Vol.2, No.1, 2011, pp.71-84. DOI: 10.5121/ijasuc.2011.2107

[14] Beth, T., Borcherding, M. and Klein, B., Valuation of trust in open networks, *Proceedings of the 3rd European Symposium on Research in Computer Security,* LNCS 875, Springer Verlag, 1994, pp. 3-18.

[15] Wang, Y., Wong, D.S., Lin, K. and Varadharajan, V., Evaluating transaction trust and risk levels in peer-to-peer e-commerce environments, *Proceedings of ISeB*, 2008, pp.25-48.

[16] Winsor, C.P., The Gompertz curve as a growth curve, *Proceedings of the National Academy of Sciences*, Vol.18, No.1, 1932, 8 pages.

[17] Molm, L.D., Takahashi, N. and Peterson, G., Risk and Trust in Social Exchange: An Experimental Test of a Classical Proposition, *The American Journal of Sociology*, Vol. 105, No. 5, Mar., 2000, pp. 1396-1427.

[18] Rao, A.R. and Bandyopadhyay, S., Measures of reciprocity in a social network, *Sankhya: The Indian Journal of Statistics*, Vol.49, series A, Pt. 2, 1987, pp.141-188.

[19] Oxford online dictionary. http://oxforddictionaries.com

[20] Jagannathan, G. and Wright, R.N., Privacy preserving distributed k-means clustering over arbitrarily partitioned data, *Proceedings of the 11th ACM KDD International Conference on Knowledge Discovery in Data Mining*, 2005, pp. 593-599.

[21] Abdul-Rahman and Hailes, S., Supporting trust in virtual communities, *Proceedings of the 33rd IEEE Hawaii International Conference on System Sciences*, 2000, 9 pages.

[22] Yan, Z. and Holtmanns, S., Trust modeling and management: from social trust to digital trust, Book chapter of *Computer security, privacy and politics: current issues, challenges and solutions*, R. Subramanian ed., IGI Global, 2007, 27 pages.

[23] Blomqvist, K., The many faces of trust. *Scandinavian Journal of Management*, Vol.13, No.3, 1997, pp.271-286.

[24] Deutsch, M., The effect of motivational orientation upon trust and suspicion, *Human Relations*, Vol.13, 1960, pp.123-139.

[25] Gambetta, D., Can we trust trust? In Gambetta, D. (Ed.), *Trust: Making and breaking cooperative relations*, 1988, (pp. 213-237), Basil Blackwell, New York.

[26] Nooteboom, Trust, opportunism and governance: A process and control model, *Organization studies*, Vol.17, 1996, pp.985-1010.

[27] Jøsang, A., Keser, C. and Dimitrakos, T., Can We Manage Trust? *Proceedings of the iTrust 2005*, LNCS 3477, Springer, 2005, pp. 93-107.

[28] Castelfranchi, and Falcone, R., Trust and control: A dialectic link, National Research Council-Institute of Psychology, Roma-Italy, 37 pages.

[29] Cofta, P., *Trust, complexity and control: confidence in a convergent world*. John Wiley, 2007.

[30] Das T.K. and Teng, B.S., Between trust and control: Developing confidence in partner cooperation in alliances, *The Academy of Management Review*, Vol.23, No.3, 1998, pp.491-512.

[31] Solhaug, Elgesem, D. and Stolen, K., Why trust is not proportional to risk, *Proceedingsof the 2nd International Conference on Availability, Reliability and Security (ARES'07),* 2007, 7 pages.

[32] Das T.K. and Teng, B.S., Trust, control, and risk in strategic alliances: An integrated framework, *Organization studies*, Vol.22, No.2, 2001, pp.251-283.

[33] Siegrist, M. and Gutsher, H., Perception of risk: the influence of general trust, and general confidence, *Journal of Risk Research*, Vol.8, No.2, 2005, pp.145-156.

[34] Estrin, D., Participatory sensing: Applications and architecture, *Proceedings of ACM MobiSys'10*, 2010, 2 pages.