Individual Opinions Versus Collective Opinions in Trust Modelling

Charif Haydar
Université de Lorraine
Laboratoire Loria, Nancy, France.
Email: charif.alchiekhhaydar@loria.fr

Azim Roussanaly
Université de Lorraine
Laboratoire Loria, Nancy, France.
Email: azim.roussanaly@loria.fr

Anne Boyer
Université de Lorraine
Laboratoire Loria, Nancy, France.
Email: anne.boyer@loria.fr

***Abstract*—Social web permits users to acquire information from anonymous people around the world. This leads to a serious question about the trustworthiness of the information and the sources. During the last decade, numerous models were proposed to adapt social trust to social web. These models aim to assist the user in becoming able to state his opinion about the acquired information and their sources based on their trustworthiness. Usually, opinions can be based on two mechanisms to acquire knowledge: evaluating previous interactions with the source (individual knowledge), and word of mouth mechanism where the user relies on the knowledge of his friends and their friends (collective knowledge). In this paper, we are interested in the impact of using each of these mechanisms on the performance of trust models. Subjective logic (SL) is an extension of probabilistic logic that deals with the cases of lack of evidence. It supplies framework for modelling trust on the web. We use SL in this paper to build and compare two trust models. The first one gives priority to individual opinions, and uses collective opinions only in the case of absence of individual opinions. The second considers only collective opinions permanently, so it always provides the most complete knowledge that leads to improving the performance of the model.**

***Keywords*—Trust modelling, Subjective logic, Recommender system, Collective trust**

I. INTRODUCTION

Web 2.0 provides a highly connected social environment. It allows data exchange among anonymous people from all around the world. Acquiring information from such sources raises the question about its reliability and trustworthiness. Modelling social trust into computational trust appeared to overcome the trustworthiness problem (for both information and resources). Today, computational trust is integrated in many domains and contexts such as social networks, recommender systems [1], [2], file sharing [3], etc.

We consider social trust as the belief of an individual, called truster, that another individual, called trustee, has the competence and the willingness to either execute a task to the favour of the truster, or to assist him to execute it. The assistance can simply be recommending another individual to execute the task. The truster tries to acquire information and constructs his own belief about the trustee before deciding to cooperate with him.

Building truster's opinion about the trustee is mainly derived by two means; the first is by exploiting previous interactions between both of them, so the truster relies on his own knowledge about the trustee (individual opinion). The second uses the word of mouth mechanism, where the truster exploits the collective knowledge of his trustee friends and their friends (collective opinion). Local trust models are those which exploit individual opinions as they are available, and collective opinions otherwise [1], [4], [2].

Our objective in this paper is to show that collective opinions can be fruitful and efficient to improve the trust based recommender system's performance even in the presence of individual opinions. We show this by comparing two trust based recommender systems: the first relies on a classical local trust model, and the second uses permanently collective opinions. Both of them are based on the subjective logic (SL) [5], which is an extension of probabilistic logic, based on the belief theory [6], [7]. SL provides a flexible framework form modelling trust.

The object of our comparison is the dataset stackoverflow [8]. It is a social website based on a question answering platform to assist users to find answers to their questions in diverse domains (programming, mathematics, English language, cooking, etc.). We assume that proposing an answer is a proof of willingness to assist the person asking. Therefore, our objective is to find the user capable to provide the most relevant answer.

The paper is organized as follows: in Section II, we present the general framework, starting by presenting social trust and computational trust. In II-B, we introduce subjective logic and some of its operators. In Section III, we describe both individual and collective trust models that we propose. In Section IV, we describe the used dataset, and present our evaluation method. In Section V, we discuss our results. Finally in Section VI, we present our conclusions and future work.

II. GENERAL FRAMEWORK

The objective of trust is to find the appropriate person to cooperate with in order to achieve a given task or context. Truster's decision about to cooperate or not is influenced by many factors such as: the context, the completeness his opinion about the trustee, the emergency of the task for him and many more. In the following section, we present a real life example about trust in order to explain this phenomena, and some factors that can influence the cooperation decision.

Suppose that Alice wants to paint her house. She publishes this information and receives three offers from three professional candidates (Eric, Fred and George) *willing* to do the job

 ISBN: 978-1-61208-312-4

for her. She already knows Eric because he painted her clinic sometime ago. Alice does not know neither Fred nor George. If Alice is satisfied by the job of Eric in her clinic, she might hire him for the house directly, and ignore the offers of Fred and George. Nevertheless, if Alice is perfectionist, she will investigate about them. Alice can ask her friends (Bob and Caroline) about Fred and George.

Suppose that Bob says that Fred is a good professional. Caroline says that she recently hired George to paint her house and she is not satisfied about his work, whereas her sister Diana has hired Fred and was satisfied. Note that even though Alice trusts Bob and Caroline, she will not ask any of them to paint her house, because she thinks that they *lack competence*. Even so, they are still capable to play an important role as advisers or recommenders.

After the suggestions of Bob and Caroline, Alice will eliminate George and choose between Eric and Fred.

In this scenario, Alice asked her friends only about the candidates that she herself does not know. The scenario could have been changed if she asked them also about Eric. Bob could say for example that Eric is good for concrete walls used in Alice's clinic, but he is not very competent for wooden walls like those of Alice's house. This information can be sufficient to convince Alice to hire Fred instead of Eric.

This example shows the limit of direct interactions manner, and that the word of mouth may be useful to enrich the knowledge of the truster about the trustee. It can lead to sharpen his decision even when he thinks that his own acquired knowledge is sufficient to take a decision.

Furthermore, this scenario allow us to distinguish four types of trust relationships; these types are also discussed in [4]:

1) Direct trust: trust is the result of interactions between exclusively the truster and trustee, such as the relations ”Alice Bob” and ”Alice Eric”.
2) Indirect trust: the two persons do not know each other. Trust is established due to trustee intermediate persons, such as the relation ”Alice Fred”.
3) Functional trust: the expectation of the truster is that the trustee accomplishes the task himself, such as the relation ”Alice Eric”, ”Alice Fred” and ”Alice George”.
4) Referential trust: the expectation of the truster is that the trustee will recommend someone to accomplish the task, such as the relation ”Alice Bob” and ”Alice Caroline”. Note that the recommendation of Caroline is also based on her referential trust in her sister Diana. In other words, no obligation for the trustee in referential trust to base his recommendation on a functional trust relation. Normally a series of referential trust relations must end with one functional trust relation [9].

Fig. 1 illustrates the trust network used by Alice to make her decision.

In the next section, we discuss the formalization of social trust for the social web, and compare the different models that exist.

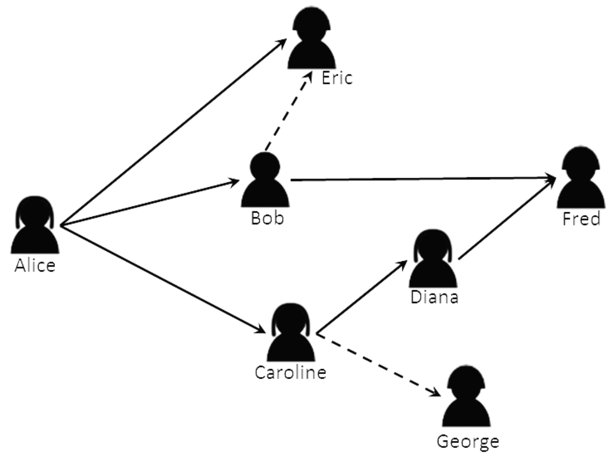

Fig. 1: Trust network

A. Computational trust

Computational trust raised in the last decade to ensure trust awareness in intelligent systems. It usually consists of a formalization of social trust adjusted to specific context and application. Basically, computational trust has three axes [10]:

- Quantitative, also called global-trust or reputation: the system computes a score for each user, this score represents his global trustworthiness. This score is considered when any other user needs to interact with this user [11].
- Qualitative, also called local-trust or relationship: it takes into account the personal bias. It is represented as user to user relationship. It is the trustworthiness of a user Y from the point of view of one single user X [11].
- Process driven (system): it represents the trust of the users in the system [10].

This work focuses on the qualitative axes. Most local trust models [1], [12], [13], [14] tend to formulate local trust problem in the form of a trust network. A trust network is a directed weighted graph where vertices represent users and edges represent trust relationships. Models differ by their notation of edges, and their strategies in traversing the network to compute trust between two unconnected users. This operation is called Trust propagation. It is fundamental in local trust models, as it allows to estimate how much a user A (called source node) should trust a user B (called destination node).

Computational trust is applied to many fields in artificial intelligence, recommender systems, file sharing, Spam detection, networks security, etc. Most computational models are fitted to their application fields and context. Basically, we identify two categories. Models dealing only with trust relationships, and models dealing with trust and distrust relationships.

The first category contains numerous models such as[15], [16], [17], [18], [19], [20]. The main disadvantage of this category is that models do not distinguish between distrusted and unknown persons. Social systems have to give chances to new and unknown users to prove their trustworthiness, whereas it must be more severe in blocking distrusted and malicious users [21]. Unknown users are often new users, a system unable to distinguish them from distrusted users risk to be very severe with them, so discourage the evolution of the trust network, or to be so tolerant even with distrusted users, so less efficient.

Models in the second category distinguish between unknown and distrusted people. Models in [22], [23], [24], [4], [25], identify three possible cases: trust, distrust and ignorance. Authors in [25] classify these models into two groups; gradual models [22], [23], [25] and probabilistic models [24], [4]. Gradual representation of trust is more similar to the human way in expressing trust, whereas probabilistic representation is more meaningful mathematically.

We use subjective logic [4], [5] (SL) in our models. Our choice is motivated by many factors. SL considers trust ignorance and distrust relationships, which is compatible with our need to distinguish between unknown and distrusted people. Most other trust models consider the creation and the evolution of trust links as an external issue, they describe and deal with existing links. SL is more transparent about this issue, trust relationships in SL are based on the accumulation of interactions between a couple of users. It proposes many operators that allow to integrate many aspects and factors of trust, which make it one of the most generic and flexible trust models.

It is based on the belief theory [6], [7] which offers the capacity to aggregate many beliefs coming from many sources (even contradictory ones), which corresponds to the case when a user has to aggregate the opinions of many friends of him about a given problem.

The following section II-B is dedicated to explain the structure and some operators of subjective logic.

B. Subjective logic

Subjective logic (SL) [5] is an extension of probabilistic logic, which associates each probability with a degree of uncertainty. Subjective logic allows to build models that treat with situations of incomplete evidences.

Belief theory [6], [7] is a special case of probability theory dedicated to treat incomplete knowledge. The sum of probabilities of possible cases can be less than 1. Subjective logic [26] offers a belief calculus using a belief metrics called opinion. The opinion of an individual U about a statement x is denoted by:

$$\omega_x^U = (b, d, u, a)$$

where: $b, d, u \in [0, 1]$ are respectively the belief, disbelief and uncertainty of U about x. The sum of the three values equals to one (i.e $b + d + u = 1$). Base rate $a \in [0, 1]$ is the prior probability. Basically, base rate is a statistical measure applied in cases of evidences' absence. For example, when we know that the percentage of a disease x in a given population is 1%, then the base rate of x's infection is 1%. When we meet a new individual who did not make a test for the disease, a priori we assume that the probability that he is infected is 1%. In social trust cases, while no a priori statistics are present, we consider that unknown person has a half chance to be trustworthy. So we use a base rate $a = 0.5$. In subjective logic, the base rate steers the contribution of the uncertainty in the computation of the probability expectation value according to 1:

$$E(\omega_x^U) = b + a \times u \tag{1}$$

The opinion in subjective logic is based on the accumulation of successful and failed experiences. After each experience, U updates his opinion about x consistently with experience's outcome. According to this description, opinion can be represented as a binary random variable. Beta distribution is normally used to model the behaviour of this kind of variables. By consequence, the opinion corresponds to the probability density function (PDF) of beta distribution. PDF is denoted by two evidence parameters α and β that can be written as functions of the number of successful and failed experiences respectively.

$$\begin{aligned} \alpha &= r + W \times a \\ \beta &= s + W \times (1 - a) \end{aligned} \tag{2}$$

where r is the number of successful experiences (evidences). s is the number of failed experiences. W is the non-informative prior weight which ensures that the prior (i.e., when r = s = 0) Beta PDF with default base rate a = 0.5 is a uniform PDF (normally $W = 2$).

The expectation value of beta PDF is:

$$E(Beta(p|\alpha, \beta)) = \frac{\alpha}{\alpha + \beta} = \frac{r + Wa}{r + s + W} \tag{3}$$

In subjective logic, the mapping between the opinion parameters and the beta PDF parameters is given as follows:

$$b = \frac{r}{(r + s + W)} \tag{4}$$

$$d = \frac{s}{(r + s + W)} \tag{5}$$

$$u = \frac{W}{(r + s + W)} \tag{6}$$

Table I shows an example of the evolution of an opinion with successive interactions.

TABLE I: Opinion evolution with successive interactions

No	state	r	s	belief	disbelief	uncertainty
0	no interaction	0	0	0	0	1
1	successful interaction	1	0	1/3	0	2/3
2	failed interaction	1	1	1/4	1/4	2/4
3	successful interaction	2	1	2/5	1/5	2/5

In the first line of Table I, we see the case of absence of evidences (experiences). The opinion is completely uncertain $(u = 1)$. In this case, according to 1, the expectation value equals to the base rate value. The arrival of new experiences, will make the uncertainty decreases, regardless if these experiences are successful or failed. Successful experiences will augment the belief, whereas failed experiences will augment the disbelief.

Subjective logic opinions can be illustrated in the interior of an equilateral triangle. The three vertices of the triangle are called belief, disbelief, and uncertainty. The uncertainty axis links the uncertainty vertex with the opposite edge (the belief-disbelief edge), the uncertainty value of the opinion is plotted on this axis considering that its contact with the edge belief-disbelief represents the value 0, whereas the contact with the uncertainty vertex represents the value 1. In the same way we describe the belief and the disbelief axis.

The opinion is represented by the intersection point of the three projections on the three axis (belief, disbelief and certainty) as shown in the example in Fig. 2. The bottom of the triangle is the probability axis, the probability expectation value is the projection of the opinion point on the probability axis with respect to the line linking the uncertainty vertex with the base rate point on the probability axis. Fig. 2 illustrates an example of opinion mapping in subjective logic. The opinion is represented by a point inside the triangle. The point is the intersection of the projection of the three values b, d, and u on the axis of belief disbelief and uncertainty respectively. the probability expectation value $E(x)$ is the projection of ω_x on the probability axis directed by the axis linking a_x with the uncertainty edge.

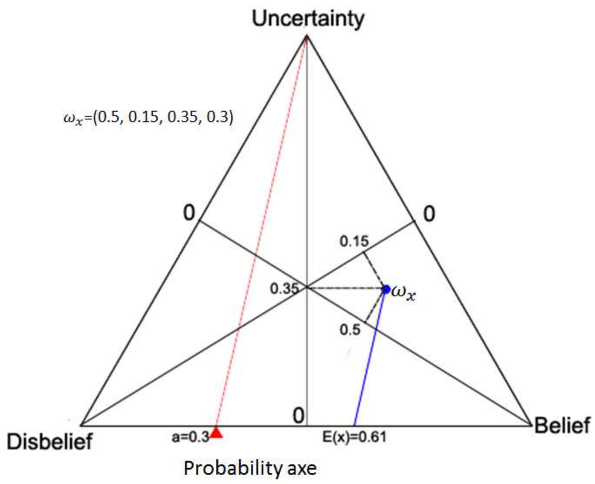

Fig. 2: Subjective logic Opinion

Note that changing the value of base rate can make people more reckless or more cautious.

After defining the structure of the opinion in subjective logic, we need to explain some of subjective logic operators that are useful for building trust network. Local trust networks are usually represented by a direct graph, where vertices represent users, and edges represent trust relations. Consequently, computing trust value between two users is reduced to finding a path or more connecting them to each other.

1) Trust transitivity: If an individual A trusts another individual B, and B trusts C, trust transitivity operator is used to derive the relation between A and C.

Subjective logic proposes the uncertainty favouring transitivity. This operator enable the user A to receive the opinion of a friend C of his trustee friend B, or to ignore the opinion of B in case of A distrust B. Formally the operator is given by 7

$$\omega_B^A = b_B^A, d_B^A, u_B^A, a_B^A$$
$$\omega_C^B = b_C^B, d_C^B, u_C^B, a_C^B$$

$$\omega_B^A \otimes \omega_C^B = \begin{cases} b_C^{A:B} &= b_B^A.b_C^B \\ d_C^{A:B} &= b_B^A.d_C^B \\ u_C^{A:B} &= d_B^A + u_B^A + b_B^A.u_C^B \\ a_C^{A:B} &= a_C^B \end{cases} \quad (7)$$

2) Opinion fusion: Suppose in the previous example that A has another trustee friend D who also trusts C. A has two separate sources of information about C.

Subjective logic proposes two main types to fuse B's and D's opinions about C:

$$\omega_B^C \underline{\oplus} \omega_D^C = \begin{cases} b_{B\diamond D}^C = \frac{b_B^C.u_D^C + b_D^C.u_B^C}{u_B^C + u_D^C - u_B^C.u_D^C} \\ d_{B\diamond D}^C = \frac{b_B^C.u_D^C + b_D^C.u_B^C}{u_B^C + u_D^C - u_B^C.u_D^C} \\ u_{B\diamond D}^C = \frac{u_B^C + u_D^C}{u_B^C + u_D^C - u_B^C.u_D^C} \end{cases} \quad (8)$$

This operator allows the user to aggregate the opinions of his trustee friends, regardless if their opinions were contradictory or not.

III. Proposed Models

The aim of our models is to predict the most relevant answer to a given question within a list of answers. Basically, trust models consider that the question owner will trust more the answers written by trustworthy people, so they try to retrieve these users. We have developed two trust aware models. Both of them use subjective logic. We refer to them as individual trust model (ITSL), and collective trust model (CTSL). ITSL is a classical local trust model, so it exploits only individual opinions when they are available, otherwise it exploits collective opinions. CTSL exploits collective opinions all the time.

A. Individual trust subjective logic (LTSL)

This model is basically based on the model proposed in [4]. It consists of building a local trust network between users. The edges of this network are SL opinions of users about each other. Formally, we represent the trust network as a graph $G = (V, E)$ where V represents the set of vertices (users), and E represents the set of edges (direct trust relationships). Suppose that a user a asks a question q, a set of users $\mathcal{R}$ will propose many answers to him. The aim of the trust model is to compute a score for each user $r \in \mathcal{R}$ using the trust network. The trust model estimates that a will accept the answer proposed by the highest score member of $\mathcal{R}$. Local trust computes the score according to 9:

 ISBN: 978-1-61208-312-4

$$score(r) = \begin{cases} e(a,r) & if\ e(a,r) \in E \\ \sum_j \underline{\oplus}[e(a,f_j) \otimes e(f_j,r)] & elsewhere \end{cases} \quad (9)$$

where: $e(a,r)$ is the direct opinion (edge) of a in r.
f_j is a member of F, the set of the direct friends of a, formally: $f_j \in F :\iff e(a,f_j) \in E$.
$\Sigma_{0 \leq j \leq N} \underline{\oplus}$ is the aggregation of multiple (exactly N) opinions. Note that $e(f_j,r)$ itself can be composed of the opinions of the friends of f_j.

In stackoverflow, when a user A asks a question, he receives a list of answers from many users. A can accept only one answer. Unaccepted answers are not necessarily bad ones. They might be simply not good enough compared to the accepted one. They even might be better but arrived too late and A has already accepted another satisfactory answer. Basically, while we do not have an explicit reaction from A towards the unaccepted answers, we suppose four hypotheses to treat them:

1) rigorous hypothesis: unaccepted answers are considered as failed interactions.
2) ignoring hypothesis: unaccepted answers are not considered at all.
3) independent subjective hypothesis: in both previous methods, the interaction value is either +1 (successful), or -1 (failed). In this method, we introduce relatively successful/failed interactions. We use the rates of community towards the answer to estimate a subjective successful/failure of the interaction. In fact, the thumb-up represents a successful interaction with an unknown user, same thing for the thumb-down with a failed interaction. The global reaction of the community towards the answer is subjective opinion resulting from members' interactions with the answer. We consider the expectation value of the community's opinion as the value of the partially successful/failure of the interaction between the person asking and the replier.
4) dependent subjective hypothesis: regarding to the fact that a user can give a thumb-up for an answer because it is better/worse than others, the attribution of thumb-up and thumb-down can be relative too. The reason why we propose another subjective method where our certainty is influenced by the global number of thumb-up and thumb-down attributed to all answers of the same question. In this case, the opinion about an answer is dependent on the the other opinions about the other answers.

$$Certainty_j = \frac{\sum_j th}{2 + \sum_{i=an_0}^{an_n} \sum_i th}$$

where th is an absolute value of thumb (up or down).
j is the current answer.
n is the number of answers of the current question.
The default non-informative prior weight W is normally defined as W = 2 because it produces a uniform Beta PDF in case of default base rate a = 1/2.

```
procedure INDIVIDUALTRUST(A, B)
    if (e(A,B) ∈ E) then
        return e(A,B)
    else
        e(A,B) ← e(0,0,1)                          ▷ a neutral opinion
        for all f ∈ A.friends do
            e(A,B) ← e(A,B) ⊕̲ [e(A,B) ⊗ e(f,B)]
        end for
        return e(A,B)
    end if
end procedure
```

Fig. 3: Individual trust function

The three components of the opinion are:

$$belief_j = uncertainty_j \times \frac{\sum_j th_{up}}{\sum_j th}$$

where $\sum_j th_{up}$ is the number of thumbs up attributed to the answer.

$$disbelief_j = uncertainty_j \times \frac{\sum_j th_{down}}{\sum_j th}$$

where $\sum_j th_{down}$ is the number of thumbs down attributed to the answer.

$$uncertainty_j = 1 - certainty_j$$

Finally we compute the expectation value of the resulting opinion and consider it as the value of the relative success/failure interaction.

To predict the accepted answer of a given question q asked by the user A, we identify $\mathcal{R}$ the set of users who contributed answers to the current question. Then, we traverse the graph (trust network) to compute the local trust between the owner of the question and each of them. We assume that A will accept the answer of the most trustee user within $\mathcal{R}$. According to this model, A consults his friends only about members of $\mathcal{R}$ with whom he has no direct interactions, otherwise considers only his own opinion. Consulted friends repeat the same strategy in consulting their friends. The drawback of this model is when A has only one interaction with a member r of $\mathcal{R}$, this might be not enough to evaluate him. A may have a friend B who has had many interactions with r so more apt to evaluate r. According to this model A will not ask B about his opinion in r.

The aim of A is to rank $\mathcal{R}$ by the trustworthiness of its members. Whenever he has no information about a member r of $\mathcal{R}$, A will ask his friends about their opinions in this very member. So the task of friends is to evaluate r without any farther information. The pseudo code 3 shows how this model works in demanding friends' opinions.

B. Collective trust

This model is based on collective opinions instead of personal opinions. In the previous model, collective opinions were used only in the case of absence of personal opinions. In this model, collective opinions are used in all cases. This

```
procedure COLLECTIVETRUST((A, R))
    Declare scores[R]
    for all score ∈ scores do score = e(0, 0, 1)        ▷ neutral opinion
    end for
    for all (r ∈ R do
        if opinion(A, r) ∈ E then
            scores[r] = e(A, r) ⊗ scores(r)
        end if
    end for
    for all f ∈ A.friends do
        fscore = collectiveTrust(f, R)
        for all r ∈ R do
            scores[r] = scores[r] ⊕ fscore[r]
        end for
    end for
    return scores
end procedure
```

Fig. 4: Collective trust function

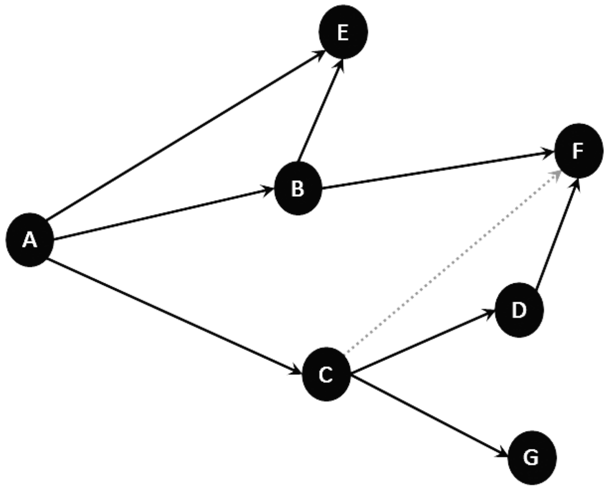

Fig. 5: Trust graph

semantically means that A will ask his friends about all the members of R, so even those who he already knows. Formally:

$$score(r) = \begin{cases} (a,r)\underline{\oplus}\sum_j \underline{\oplus}[e(a,f_j)\otimes e(f_j,r)] \\ \quad if\ e(a,r)\in E \\ \sum_j \underline{\oplus}[e(a,f_j)\otimes e(f_j,r)] \\ \quad elsewhere \end{cases} \tag{10}$$

This model assumes that direct interactions are frequently unable to assure sufficient information about users. In the previous model, user could supply a personal opinion about another user once he has at least one interaction with him. We think that this affects the quality of the opinion, because of the lack of experience. In the current model, user aggregate his opinion with the his friends' opinions, each friend's opinion is conditioned by the trust given to him by the active user.

Example:

Back to the same example in Section II. Fig. 5 illustrates trust network extracted from the described relations in the example. So when A asks a question to which she get replies from E, F and G, then $\mathcal{R} = E, F, G$. A needs to rank the members of $\mathcal{R}$ to identify the most trustworthy member.

For the individual trust model, scores are computed as follows:

score(E)= e(A,E)

score(F)= [e(A,B) $\otimes e(B,F)]\underline{\oplus}[e(A,C)\otimes e(C,D)\otimes e(D,F)]$

score(G)= e(A,C) $\otimes e(C,G)$

As for the collective trust model, the scores of F and G do not change, but the score of E becomes as follows:

score(E)= e(A,E) $\underline{\oplus\ [e(A,B) \otimes e(B,E)]}$

Now let us add a link between C and F, and see the effect of such a link:

In individual trust model:

score(F)= [e(A,B) $\otimes e(B,F)]\underline{\oplus}[e(A,C)\otimes e(C,F)]$

In collective trust model:

score(F)= [e(A,B) $\otimes e(B,F)]\underline{\oplus}[[e(A,C) \otimes e(C,F)]\underline{\oplus}[e(A,C)\otimes e(C,D)\otimes e(D,F)]]$

Once again, we see that in individual trust model, when A asks C about his opinion in F, as C has a direct link with F, he his response to A is based only on this direct link. Whereas in collective trust model, for the same case, C asks D about this last's opinion about F, and return to A the aggregation of the opinion D conditioned by the trust between C and D, and C's own opinion.

IV. EXPERIMENTAL WORK

We use the dataset of the website stackoverflow. The website offers a question answering forum for multiple domains, mainly but not limited to computer science. The available data contains 30 domains. Users subscribe to the website by domain, so one user can have multiple accounts, according to the number of domains in which he participates. The total number of accounts is 374,008 for about 153,000 users.

The user asks a question in a given domain, and associates a set of keywords to his question, then he receives many answers. He chooses the most relevant answer to him and attributes an "accepted answer" label to it. Nevertheless, users can keep proposing new answers. Subsequent users who have the same problem as the person asking can take advantage of the answers and rate them on their usefulness by attributing thumb-up or thumb-down. In the available dataset, we have access to only the total number of thumbs-up and the total number of thumbs-down an answer has, but no information about suppliers' identities. The website, offers the possibility to order answers by relevance, where the accepted answer is put in the top of the list, followed by the other answers ordered by the difference between thumbs-up count and thumbs-down count. Our work aims to use trust based models to predict the accepted answer over the set of available answers. Total number of questions in current dataset equals to 371,594, for a total number of answers 816,487. We divide the questions of each domain in five equivalent sets. Then, we apply a crossing test in five iterations, in each iteration we use four sets for learning and building the trust network and the fifth for testing the prediction quality.

Evaluation Metrics

We consider the problem of finding the accepted answer as a list ranking problem with one relevant item. Mean reciprocal rank (MRR) is a quality metrics used to evaluate systems that have to give out a ranked list with only one relevant item. Reciprocal rank (RR) of question is $1/r$ where r is the rank given by the evaluated algorithm to the accepted answer. Mean reciprocal rank is the mean value of RR's to all questions. The value of this metrics varies between 0 and 1, where 1 is the best precision score.

MRR is a good indicator to the performance of prediction algorithms for ranked lists. Nevertheless, we think that it is not perfectly adapted to our case. MRR is usually used for systems that have to predict a list of items within which a relevant item exists. We are trying to find the accepted answer by re-ranking an existing list of answers. Remark the case when the algorithm ranks the relevant item in the last position of the list, the algorithm is recompensed for at least having chosen the item within the list. In our case, the list is predefined, so the algorithm should not be recompensed for ranking the relevant item at the end of the list. The range of RR values is $[1/r, 1]$, we propose a modified version where the value varies between 1 if the relevant item is in the top of the list, and 0 if it is at the end of the list. We call this metrics mean predefined lists rank (MPLR), where predefined lists rank PLR is given by the formula:

$$PLR = \frac{N - r}{N - 1}$$

where: N is the size of the list.

MPLR is the average of PLRs for all questions. We employ a modified competition ranking strategy, so the ranking gap is left before the *ex aequo* items. For example if two items on the top of the list have the same score, they are considered both second, and no item is put at the top of the list.

V. RESULTS AND DISCUSSIONS

Only questions with accepted answer and more than one proposed answer are appropriate for our test. The corpus contains 118,778 appropriate questions out of the 371,594 questions of the corpus.

Table II illustrates the MRR scores of both models, and table III illustrates MPLR scores. MPLR scores are, of course, lower than those of MRR. Nevertheless both tables lead to the same conclusions.

It is obvious that the collective trust has a considerably better performance than individual trust on this dataset. This is because of collective opinions that rely on more complete evidences than individual ones. Trustee friends enrich collective opinions by more knowledge that leads them to be more reliable and accurate than individual ones. These results show the limit of individual opinions and local relationships, because direct interactions can be poorly informative, and relying only on them can lead to inaccurate decisions. An individual in a social environment needs always to integrate and interact within communities to be more informed, and more capable to adjust his decisions.

TABLE II: MRR results

method	Individual trust SL	Collective trust SL
Rigorous	0.57	0.88
Ignoring	0.58	0.75
Dependent probabilistic	0.62	0.87
Independent probabilistic	0.617	0.86

TABLE III: MPLR results

method	Individual trust SL	Collective trust SL
Rigorous	0.37	0.85
Ignoring	0.36	0.69
Dependent probabilistic	0.442	0.84
Independent probabilistic	0.438	0.83

In real life, regret can assist to re-establish trust. The structure of local trust systems does not possess any mechanism to reconsider relationship after a bad integration with a destination user (which can be occasional), collective opinions allow the reconsideration of the relation with this user if he was trustee by intermediate friends of source user.

Regarding the four hypotheses about treating unaccepted answers in individual trust, we find that probabilistic methods are slightly better than both rigorous and ignoring hypotheses. In the collective trust model, the three hypotheses that try to infer from unaccepted answers surpass the performance of the forth that neglects these information (ignoring hypothesis). We conclude that unaccepted answers can be profitable, and then should not be neglected. Extracting information from these answers is possible thanks to the flexibility of subjective logic. This framework proves again its capability to deal with incomplete evidence cases.

On the other hand, in global trust, all users contribute in evaluating the trustworthiness of each user. A unique score is attributed to each user. The score is based on all his interactions (as trustee), so a source user can access more information about the destination user (compared to collective trust). The disadvantage of global trust is its weakness against malicious group attack. If a group of malicious users cooperate to highly rate each other they can improve their reputation score and disturb the system [27].

Collective trust model can provide source users with more information about destination users compared to local trust, and it controls who can participate in computing the score of destination user. Theoretically, collective trust model is more resistant to group attack compared to global trust model. In addition, collective trust is user biased, this means that a destination user has not the same score every time, and that the score is dependent to the source user too.

VI. Conclusion and Future Works

We showed in this paper the superiority of collective opinions over individual ones in a trust model. They are usually more complete, reliable and informative. So, depending on them, it leads the user to take more robust decisions.

The model proposed lies between local and global trust. Collective trust supplies its users with more complete information than classical local trust. Besides, it relies, theoretically, on more trustworthy information than global trust.

The first argument was proven experimentally on real dataset in this work. Our future work will focus on comparing the performance of a collective trust model and global trust model, when injecting malicious group attacks in the dataset.

References

[1] P. Massa and B. Bhattacharjee, "Using trust in recommender systems: an experimental analysis," *Trust Management*, p. 221235, 2004. [Online]. Available: http://www.springerlink.com/index/TFCG7W34VF58YAWL.pdf

[2] J. A. Golbeck, "Computing and applying trust in web-based social networks," Ph.D. dissertation, University of Maryland at College Park, College Park, MD, USA, 2005, AAI3178583.

[3] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in P2P networks," in *Proceedings of the 12th international conference on World Wide Web*, ser. WWW '03. New York, NY, USA: ACM, 2003, p. 640651. [Online]. Available: http://doi.acm.org/10.1145/775152.775242

[4] A. Josang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," in *Proceedings of the 29th Australasian Computer Science Conference-Volume 48*, 2006, p. 8594. [Online]. Available: http://dl.acm.org/citation.cfm?id=1151710

[5] A. Josang. (2013, Sep.) Subjective logic. [Online]. Available: http://folk.uio.no/josang/papers/subjective_logic.pdf

[6] A. Dempster, "The DempsterShafer calculus for statisticians," *International Journal of Approximate Reasoning*, vol. 48, no. 2, pp. 365–377, 2008.

[7] R. R. Yager, J. Kacprzyk, and M. Fedrizzi, Eds., *Advances in the Dempster-Shafer theory of evidence*. New York, NY, USA: John Wiley & Sons, Inc., 1994.

[8] (2013, Sep.) Stack overflow website (data collected in sep 2011). [Online]. Available: http://stackexchange.com/

[9] A. Josang and S. Pope, "Semantic constraints for trust transitivity," in *Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling-Volume 43*, 2005, p. 5968. [Online]. Available: http://dl.acm.org/citation.cfm?id=1082284

[10] M. Kwan and D. Ramachandran, "Trust and online reputation systems," in *Computing with Social Trust*, ser. HumanComputer Interaction Series, J. Golbeck, Ed. Springer London, Jan. 2009, pp. 287–311. [Online]. Available: http://link.springer.com/chapter/10.1007/978-1-84800-356-9_11

[11] C. N. Ziegler and G. Lausen, "Spreading activation models for trust propagation," in *e-Technology, e-Commerce and e-Service, 2004. EEE'04. 2004 IEEE International Conference on*, 2004, p. 8397.

[12] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000*, Jan. 2000, p. 9 pp. vol.1.

[13] K. Krukow, *Towards a Theory of Trust for the Global Ubiquitous Computer: A Dissertation Presented to the Faculty of Science of the University of Aarhus in Partial Fulfilment of the Requirements for the PhD Degree*. Department of Computer Science, University of Aarhus, 2006.

[14] L. Mui, *Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks*. PhD Thesis, Massachusetts Institute of Technology, 2002. [Online]. Available: http://www.cdm.lcs.mit.edu/ftp/lmui/computational%20models%20of%20trust%20and%20reputation.pdf

[15] W. Tang, Y.-X. Ma, and Z. Chen, "Managing trust in peer-to-peer networks," *Journal of Digital Information Management*, vol. 3, no. 2, p. 58, Jun. 2005. [Online]. Available: http://www.questia.com/library/1G1-186470835/managing-trust-in-peer-to-peer-networks

[16] M. Richardson, R. Agrawal, and P. Domingos, "Trust management for the semantic web," in *In proceedings of the second international semantic web conference*, 2003, p. 351368.

[17] I. Zaihrayeu, P. P. D. Silva, D. L. Mcguinness, I. Zaihrayeu, P. Pinheiro, S. Deborah, and L. Mcguinness, "IWTrust: improving user trust in answers from the web," in *Proceedings of 3rd International Conference on Trust Management (iTrust2005*. Springer, 2005, p. 384392.

[18] R. Falcone, G. Pezzulo, and C. Castelfranchi, "A fuzzy approach to a belief-based trust computation," in *Lecture Notes on Artificial Intelligence*. Springer-Verlag, 2003, p. 7386.

[19] F. Almenrez, A. Marn, C. Campo, and C. G. R, "PTM: a pervasive trust management model for dynamic open environments," in *First workshop on pervasive security, privacy and trust PST04 in conjuntion with mobiquitous*, 2004.

[20] J. O'Donovan and B. Smyth, "Trust in recommender systems," in *Proceedings of the 10th international conference on Intelligent user interfaces*, 2005, p. 167174. [Online]. Available: http://dl.acm.org/citation.cfm?id=1040870

[21] R. Burke, B. Mobasher, R. Zabicki, and R. Bhaumik, "Identifying attack models for secure recommendation," in *Beyond Personalization: A Workshop on the Next Generation of Recommender Systems*, 2005. [Online]. Available: http://maya.cs.depaul.edu/mobasher/papers/sp-iui05.pdf

[22] M. De Cock and P. P. da Silva, "A many valued representation and propagation of trust and distrust," in *Proceedings of the 6th international conference on Fuzzy Logic and Applications*, ser. WILF'05. Berlin, Heidelberg: Springer-Verlag, 2006, p. 114120. [Online]. Available: http://dx.doi.org/10.1007/11676935_14

[23] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of trust and distrust," in *Proceedings of the 13th international conference on World Wide Web*, 2004, p. 403412. [Online]. Available: http://dl.acm.org/citation.cfm?id=988727

[24] U. Kuter and J. Golbeck, "Using probabilistic confidence models for trust inference in web-based social networks," *ACM Trans. Internet Technol.*, vol. 10, no. 2, p. 8:18:23, 2010. [Online]. Available: http://doi.acm.org/10.1145/1754393.1754397

[25] P. Victor, C. Cornelis, M. D. Cock, and P. P. D. S. B, "Gradual trust and distrust in recommender systems. fuzzy sets and systems," in *In press*, 2009.

[26] A. Josang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 03, p. 279311, 2001. [Online]. Available: http://www.worldscientific.com/doi/abs/10.1142/S0218488501000831

[27] B. Mobasher, R. Burk, R. Bhaumik, and C. Williams, "Toward trustworthy recommender systems an analysis of attack models and algorithm robustness.pdf," vol. 7, no. 4, 2007. [Online]. Available: http://doi.acm.org/10.1145/1278366.1278372