Trust Management in social networks

Talel Abdessalem, Bogdan Cautis, Asma Souhli

Télécom ParisTech, LTCI – UMR CNRS 5141

46, rue Barrault – 75013 Paris – France

First.Last@telecom-paristech.fr

ISICIL Project - ANR 2009

October 23, 2009

CONTENTS

I. Introduction

The web 2.0 enables users to get information, obtain services and communicate with others in new ways. As a consequence, it reconfigures access not only to information and services but also to people: who a user knows, trusts and stays in touch with. Some of the most exciting new activity on the web is social, with social networks and collaborative interaction. In a few words, these are applications that allow users to share items (such as photos, movies, documents, bookmarks, scientific citations, blog pages, slides, and so forth) and to assign descriptive terms from an uncontrolled vocabulary (denoted tags) to items of their interest.

The open and decentralized nature of the web raises challenging issues such as the protection of rational users against malicious ones. This issue arises in various areas as e-commerce (where users are to be protected against product marketers disinformation), e-services (where users are to be protected against spamming) and on-line forums and social networks (where users are to be protected from misinformation with respect for example to age and gender). For all of these areas, trust is a critical issue as it highly impacts person's decision to go on-line, what to do on-line and with which persons.

The problem of managing trust in an open and centrialized/decentralized system has attracted substantial research efforts in recent years [12], [3], [17], [5], [8]. A commonly used solution to tackle the problem of trust management is to build a "web of trust". In a "web of trust", each participant is allowed to express the degree of its trustworthiness in others. By doing so, a participant helps the other in deciding which participants are to trust or to distrust, without prior interaction [7].

Current work in the area of trust management in a "web of trust" can be classified into two families. Approaches of the first family infer trustworthiness by propagating trustworthiness from a participant to another. Approaches of the second family infer trustworthiness by machine learning from prior interactions of a user and are called *predictive*.

This report surveys and compares the main approaches studying trust and trust inference in social networks. In particular, the report highlights key trust inference issues and provides insights into the factors shaping trust in a "web of trust". We present a personal point of view on how to structure the different concepts related to trust calculation. In other words, we try to organize the different encountered insights in order to define a mechanism taking into account all relevant and necessary factors for trust inference in a network. We turn thereafter to the description of our proposed model as an extension of the *direct propagation* proposed

in [7]. A second contribution is also detailed based on a *predictive* way in generating a weight that subjectively reflects the importance of each type of propagation for a user, learned from its own decisional trust assignment background

The remainder of the report is organized as follows. Section II and III present the state of the art: the trust management key issues and the two major directions for computing the trust between users. In Section IV we discuss and present the proposed model. The experimental dataset (Epinions community, *epinions.com*), the algorithmic steps and the experimental phases are then detailed, followed in section V by a discussion on the perspectives of this work. Then, section VI concludes this report.

II. Trust Management

Intuitively, computing trust requires some indicators such as information about the reputation of a given user. By reputation, we mean the level of trust assigned by the community (or part of the community) to the target node. This can be expressed according to the rating process used in several sites such as eBay, or a statement of trust as in the case of Epinions.

In some computing approaches based on the exploration of the trust network structure, knowledge of the existing trust relations (trust ties of the graph) is important to establish the required relationship between two given users.

The first part of this section describes politics to hold trust on centralized/decentralized architectures. The second part lists the different trust models, such as binary or more generally discrete models (a discreet scale of possible trust values), the probabilistic model, fuzzy model with error margins, etc.

A. Architectures

In JøsangŠs "Trust and reputation systems" paper, two architectures of trust and/or reputation networks were specified: centralized and decentralized systems. In fact, in centralized systems all the scores, information and values of trustworthiness that a user A gave to a user B are collected in a central authority. Therefore, a value of reputation given to a user may be assessed from the different scores given by other users relating to the same context. This evaluation requires user A to check the reputation centre about the B's reputation score. Thus, as information is publicly accessible for any participant in the system this may yield privacy concerns. Still, Ziegler and Lausen (2005) [18] notified that online communities using a web of trust require their users to disclose all trust information to the community server, but not

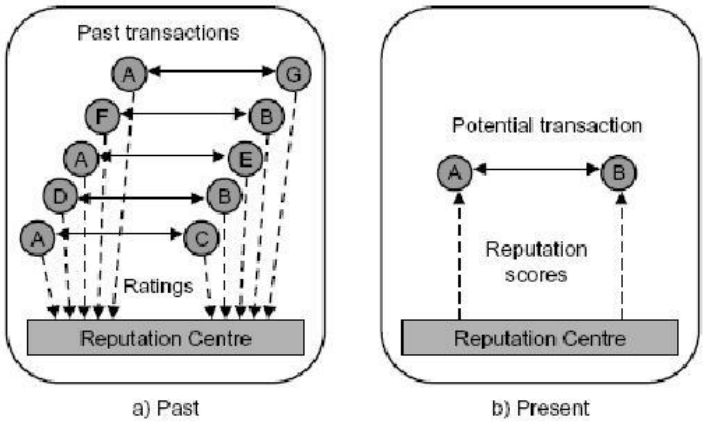

Fig. 1. General framework for a distributed reputation system [11]

necessarily to other peers [7]; privacy is however maintained. Concerning social networks, we classify them under centralized architecture (figure 1).

In a different type of application, as mobile ones for instance, the distributed architecture is deployed. Using such devices, computing trust one can give to another user would be benefic in sharing digital content to avoid swamping by malicious ones. Users may organize content producers that they know and trust in a web of trust [16]. Figure 1 shows that in a distributed environment, each participant is responsible for collecting and combining ratings from other participants [11].

B. Trust Models

Generally, individuals express their trust through a percentage and less commonly with an absolute value. However, depending on the interactions nature of relations between individuals in a community, a meaningful way to represent the value of trust is properly designed.

1) Discrete Trust Models: Expressing trust in a scale of discrete data is easier to interpret in general that the probability statements which require greater figuring cognitive effort: It would be simpler to say that a user is "usually trusted" rather than expressing such statement as a percentage like trusted in 70% of cases [11]. A community such as Epinions (*epinions.com*) uses a binary scale for the expression of trust: a user declares his trust in another (confidence) performed by the positive value of 1, or distrust by choosing the option of blocking that user and this would be interpreted as the negative value -1. The zero (represented on the graph of the network) indicates that there is no declared relationship yet trust between the two users. Computation of trust would eventually generate continues values, as it is the case in [7];

however, techniques for rounding the results within the followed scale are then introduced.

2) Probabilistic Trust Models: The main advantage from expressing trust with probabilities would be the possibility of applying probabilistic methods from simple models based on probability calculus to models using advanced statistical methods, as they are very robust in terms of treatment such as Bayesian approaches or models for reasoning through Markov chains (e.g.; [15]). Even in a system of discrete values, the calculation methods include estimation of relationships that may be relevant in determining the value of trust. These indices will participate with a certain weight in the trust value generation that the system will propose. Thus, the probabilistic approaches can also be operated and the trust resulting value would be a continuous value proposed to the user helping for making his decision on whether trusting or not a different target user.

3) Belief Models: In such models, trust may be represented by a system holding a continuous value of trust, distrust and the uncertainty. The sum of its values can be determined to 1 as in opinions Belief Models proposed by Jøsang (1999, 2001) in [9] and [10]; it could not cover the area of belief and be less than 1. The tree values are then considered by the computing design and semantics of each participate in determining the result of system values. Combining trust and distrust to represent the belief of a user at a given instant bring the model back to a belief model. This aspect appears in the propagation model of trust and distrust in [7] where a Belief matrix is set up combining all pairs of users' beliefs towards each other, a belief value that aggregates the portion of trust and distrust that a pair assigns to another.

4) Fuzzy Models: Fuzzy logic is suitable for trust evaluation as it takes into account the uncertainties in expressions used to determine the trust. Many works like [4] and [1] propose a trust model for multi-agent system using fuzzy sets. Samia Nefti and al [14] present a method based on fuzzy logic to evaluate trust in Ecommerce arguing that fuzzy logic is suitable for trust evaluation as it takes into account the uncertainties within E-commerce data and like human relationships, trust is often expressed by linguistics terms rather then numerical values.

III. Computing Trust

Mainly, we can distinguish two different approaches to calculate the trust value expected between a pair of users. The first approach would be the propagation of values of trust through consecutive users' trust relations in the graph following an effective trust path leading to the

target user. The second approach arises from the philosophy of analyzing users' behaviors in a given social community to trace the causes that may appear behind the establishment of a trust relationship.

A. Propagating Trust

We begin by introducing most relevant tracks identified trough different studies leading to propagation over the trust graph of a typical social network. In other words, we lay out the situations where the propagation to a third user is possible. To further enhance the probability of propagation, we next introduce some factors identified through a semantic analysis of existing links (initial structure graph portion) reflecting a user's behavior, which could had influenced his decision of assessing the trust.

1) Potential Transitions: Before introducing types of transitions that could be concluded to propagate a value of trust between users, we clarify that the following mechanisms are applicable only to relations on the same utility (i.e., the context of trust, for instance: recommending films, repairing cars, baby sitting service, etc.). For this reason, we assume that the graph ties are annotated with the utility that determines the specific context of each interaction.

Consider the given part of a web of trust in Figure 2 through which we illustrate the different possibilities of trust propagations (transitions) between users A and F. Lets begin with transitivity, which is the simplest and most intuitive type of transition that could be applied: Given a user A having a direct connection with a user D as shown in Figure 2 (A and D interact together so that a specific level of trust exists between them, given the supported quantification model). The idea of transitivity is about the evaluation of a trust level that A may hold towards a third user F in whom D trusts.

The transitivity is far from being systematic given the strong subjectivity characterizing such relationships. In a coming section, we point out conditions or more accurately factors on which this propagation and the following ones strongly depend; for example, taking in consideration the capacity of Bob to recommend people for a given utility, a value that Alice assigns to him (*dr-trust*, direct recommendation trust as shown in figureTDTT). We will also describe some existing methods for calculating such factors. R. Guha et al. [7] name transitivity propagation "Direct propagation" or "atomic propagation" as it is the most intuitive. Besides, they introduce some reflections on the possibility of establishing relations between users, apart from the direct spread.

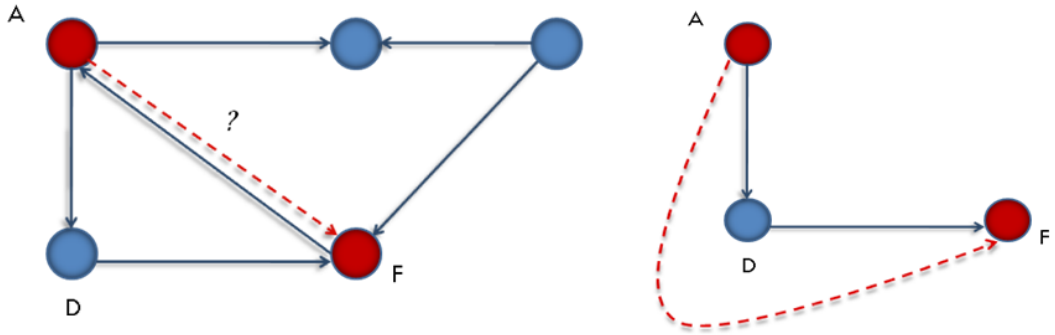

Fig. 2. Trust propagation (the dotted line indicates the trust to infer)

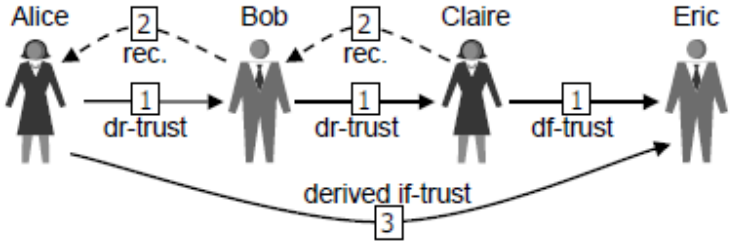

Fig. 3. Trust derived through transitivity [11]

An intuitive and very basic formula for calculating the transitive propagation of trust would be as follows:

$$T_{1\to N} = \frac{\sum_{i=1}^{N-1} \mu_d T_{i\to i+1}}{N-1},$$

where N denotes the number of steps and μ_d a discounting factor [6], which decreases as i increases to penalize the lengthy paths.

Referring to the right side of Figure 4, we can more or less conclude that if two users A and C have a common trusted third B (always in the context of a given utility), then one may likely trust the non common nodes, as an example, we may expect A to develop a value of trust toward F as he is trusted by C. This type of transition is named "co-citation propagation".

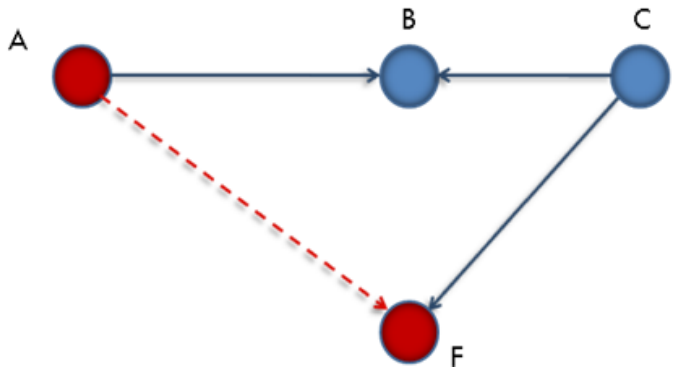

Fig. 4. Co-citation propagation [7]

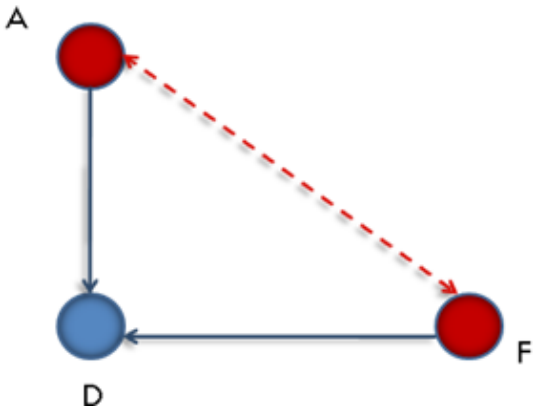

Fig. 5. Trust Coupling relationship

Such mechanism still depends also on conditions reflecting the user's subjectivity, such as A's reasoning, to let the co-citation propagation occur. This point will be discussed later when introducing methods for computing such factors, whose role is to simulate the causes behind participant's subjectivity. Likewise, as A and F trust the same person(s) (see figure 5), they should trust one another as A's trust in D should propagate to F and the same conclusion should be induced from F's side as well. We perform in this way the "Trust Coupling" [7].

Another track for the Propagation of trust would be the possible transposition that a direct relation from A to F may hold (see figure 6). In other words, if I trust someone and explicitly express my trust in him, he may intuitively begin to develop a sense of trust in return. This is called "Transpose Trust" [7].

2) Determining Factors for Trust Propagation : In this section, we detail some studied methods for computing reliable indicators (informers). Based on such values, we can determine a mechanism to evaluate users' behavior toward others in the network; an evaluation

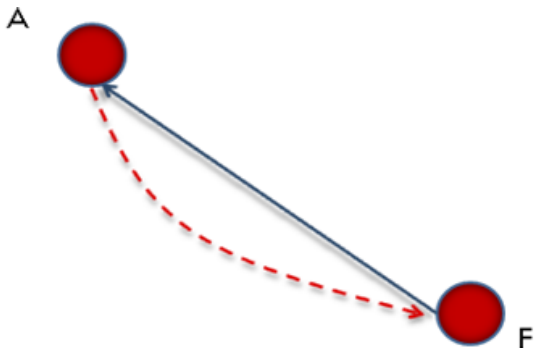

Fig. 6. Transpose Trust relationship

which will allow getting closer at most to the subjectivity determinants of a user. Hence, these factors would allow concluding relevant trust relationships and must be included in the computing process.

We note nevertheless that besides the "derived factors" (presented in further sub-sections), the "direct" ones, just as the given value of trust that A assigns to D and that D assigns to F for the transitivity for example (where the trust relationship between A and F is to be determined), are given as the initial indicators for a global formula of calculation taking all factors into account.

We assume that a user would like to have estimation on the level of trust that he may have toward another user with whom he never interacted before. The transitivity is not always systematic, even if we are still speaking for the same utility. Indeed, A could judge that D is different from him concerning the recommendation of other users even if A trusted him. We must therefore distinguish between giving trust level and capacity of recommendation that A grants to D. We translate this with the example of movie preferences: Suppose Anja trusts Pierre for the recommendation of films. She finds that they generally have the same preferences. On the other hand, Pierre trusts Eric as they share a same preference for one single movie which is the all-time favorite one for Pierre, and based on which he judges Eric as trustworthy. Hence, such relation is established based on very subjective assessment. To spread the trust to Eric, Anja must first evaluate the relevance of the recommendations of Pierre, and assess the likely rate of resemblance between Pierre and Eric.

a) Ability to Recommendation: The authors in [16] identify a factor (Judging relationship) which evaluates the difference between the trials of two users towards common nodes. They use it as an indicator for predicting the trust instead of propagating it. We introduce it in this section as a factor for wielding the propagation and have a look back on the judging

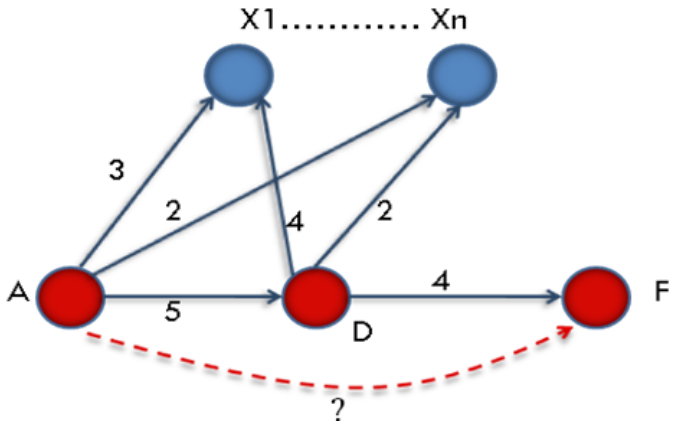

Fig. 7. Judging relationship.

relationship as a predictive indicator in the coming section. At this stage, we adopt the discrete model (or the probabilistic one) which allows rating a user by assigning a discrete value of trustworthiness from a predefined scale of possible values of trust. The littler is this value the lower is trust. A method in [16] for calculating the similarity factor reflecting the resemblance in judgments proceeds as follows: for any X^i rated by users A and D (A $\rightarrow$ X^i and D $\rightarrow$ X^i), we calculate the absolute difference between the two values of trust and then aggregate all the values calculated for each X (see figure7). For instance, we can use the average as an aggregation function. Therefore, to better reflect the variance between the differences, the authors in [16] consider a second way of aggregating that accounts for both number of differences and their variance: to compute the confidence interval of the average (with 95% of confidence) and take the higher extreme. They also evaluate which aggregation leads to the highest accuracy.

Distrust is not yet studied at this level of our synthesis. Otherwise, its value should be taken into account as it may reflect incertitude towards D (predefined tolerance) which can influence the derived recommendation rate B (e.g., to reflect the impact of D's trust on users judged doubtful or untrustworthy by A).

This factor may be integrated in the final global formula of computing the concluded relation of trust between tow given nodes. For example, if we consider only the formula taking into account the transitivity derivation of trust, an additional recommendation factor μ_{rec} wielding the propagated value comes as follows:

$$T_{1\rightarrow N} = \frac{\sum_{i=1}^{N-1} \mu_d \mu_{rec} T_{i\rightarrow i+1}}{N-1},$$

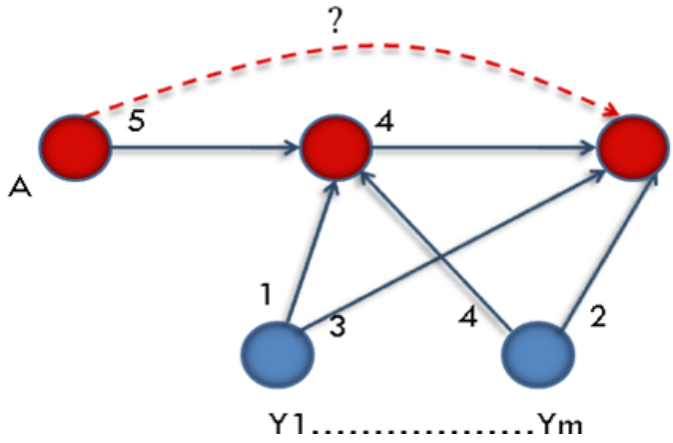

Fig. 8. Approximation of users

Therefore, this factor would have a weight in the formula reflecting its importance as a subjectivity indicator.

b) Approximation of Users: Still, we can find ourselves in a situation where there is no path to the node for which a potential trust value is looked for. In such a case, a similarity factor between the tendencies of the initial node and the target node must be determined. One way to calculate this factor would be by aggregating the differences. Again, the author in [16] introduce it as a predictive indicator for trust. Still, we may expose it as another determining factor of propagation at this level. Given A rating D (A→D), we seek an approximation of the rating that would be given to F (A → F).

For this sake, intuitively D and F's performances should be compared: the more the performances are similar the more likely the value assigned by A to D would be close to that to assign to F. The method outlined in [16] evaluates this similarity by aggregating the differences between the ratings of different nodes assessing both D and F: the more this value is smaller the more D and F are similar. Note however that this calculation is derived from the reputation score of a given node and requires a centralized context (the statement in [16], which provides a procedure for calculating the propagation of trust in a decentralized context, is settled for calculations returned by the number of nodes that have revealed their assignments).

This would be an alternative way for assessing a level of trust in the absence of a propagating path in the graph. In all cases, it could be integrated (with a given weight) in the overall trust propagation formula and would be an additional refining factor μ_{app}, with possibly a related weight:

$$T_{1\to N} = \frac{\sum_{i=1}^{N-1} \mu_d \mu_{rec} \mu_{app} T_{i\to i+1}}{N-1},$$

c) Global Reputation: The approximation of user leads us to talk about the reputation of a node that could be held in a community. In a centralized system, the reputation of a user is determined by trust average ratings provided by the users for that node [2]. The reputation of a user could be a significant indicator for determining the trust value assigned from one user to a another. An example of online sales sites like E-Bay and Amazon, adopt the policy of raking suppliers, which, amongst other things, determine the preferences of users and assesses the reputation of suppliers. In some communities, as stated in [2], the data published and shared or activities require some level of privilege for access. Thus it is noted that a user with a level of access to highly privileged information will be more likely to have a good reputation in the network. The authors in [2] call this score the effective trust.

d) Distrust: Several studies, where [7] is among the firsts, introduced mathematical approaches to distrust quantification and propagation. The importance of distrust propagation arises by a third option in few trust-systems such as Epinions and eBay through which a user can manifest its distrust towards another by blocking him for example, beside classical options for expressing his trust in another (binary value 1). The zero value comes to reflect an initial state between any pair of users where no value of trust/distrust is yet revealed. In [16], the authors make the assumption that in this scale 0,1 a third value expressing the distrust can be integrated. However, reviewing the specification of the approach is necessary to ensure a generation of coherent values. In [7], the authors discuss the possibility of depicting distrust through a negative value which might deteriorate the results as the expression of distrust is more informative than the trust in some cases. Their specification, therefore, adopts initial binary matrices for trust and distrust and a global Belief matrix combining the two to hold the state of the world at an instant t: B^{ij} is the value of trust that relates i to j, or the value of trust combined with distrust relating i to j. A generic operation is then defined and can be applied to trust alone (T), to trust combined with distrust (typically, T - D).

e) Semantic Relatedness: We also pointed out that in a community where the trust assignment is made for a precise context any type of propagation is performed trough a same utility connections. If the system offers a generic function for users to annotate their trust connections, we may find ourselves facing the issue of normalizing the annotations. As users are free to annotate their aim of trust assigned to others, it is frequent that each use

a different expression to define the trust context. For instance, Alice may annotate her trust to Eric as a good informer about greenhouse effect issues using the annotation:"Greenhouse effects". Pierre, from his side could annotate his similar connection as "Global warming: Greenhouse gas ". We can see that a lexical based propagation is not robust enough as using different expressions with same semantic meaning is highly inconvenient and could prevent the propagation to happen. In stead, we propose considering the whole network with all possible context trust connections using a semantic bridging of the different utilities when seeking the best leading path(s) to the target node. The semantic distance is therefore computed to return a semantic weight to be added to the transition computing formula. This additional weight would reflect the level of terms accuracy and would be an efficient same-context propagation "watcher". For instance, adding the semantic weight μ_{sem}, the transitivity formula becomes:

$$T_{1\to N} = \frac{\sum_{i=1}^{N-1} \mu_d \times \mu_{rec} \times \mu_{app} \times \mu_{sem} \times T_{i\to i+1}}{N-1}$$

Many semantic switchers are implemented; we can refer to the study of Rudi Cilibrasi and Paul Vitanyi in [21] that details a method to automatically extract the meaning of words and phrases from the world-wide-web using Google page counts.

3) Models for Computing trust Propagation: The propagation mechanism set by R. Guha et al. relies on a matrix representation of the network. Each type of transition (see figure 9) returns a value participating with a certain weight in determining the value of trust between a pair of users.

$$T'_{A\to F} = \mu_1 DP \times \mu_2 TC \times \mu_3 CC \times \mu_4 TT$$

where:

- DP denotes Direct Propagation, using the identified transitivity transitions through the target node's leading path.

- TC denotes Trust Coupling, aggregation of all the possible trust coupling links that could happen between A and F.

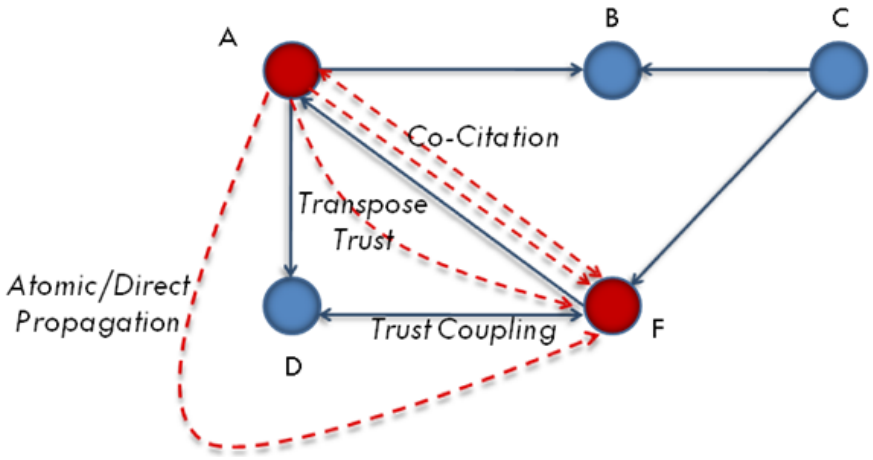

Fig. 9. The different transitions of trust between a pair of users

- CC denotes Co-Citation, aggregation of all the possible co-citation links that could happen between A and F.

- TT denotes Transpose Trust that could be between A and F.

- μ_1, μ_2, μ_3, μ_4 are successive weights given to each type of propagation transition, switched through experiments and fixed relatively to the best results.

For each type of transition, a matrix of Trust (or Belief B, if it is a combination of trust and distrust) is established. If the network consists of N users, the matrix would have a $N \times N$ dimension. Over a series of iterations, the belief matrix would behold new values derived from exploring each possible type of transition that could be found between each pair of users. As instance, the operator applied to the trust through transitivity is the matrix B itself which leads to $B \times B = B^2$ in the first iteration.

The final state of the matrix represents the values of derived trust generated through each type of transition. Note that in the end of every iteration the matrix B is updated by the addition of the values generated in the resulting B^i (obtained in the i^{th} transition) with respect to weights given to every type of propagation.

Obviously, it is expensive and computationally not robust towards scalability as randomness in links increases and lots of same length paths would be available. Spread is highly related to the context and the subjective intentions of users, a reason behind which the authors in

[7] did not set a standard method of propagation, but have developed several methods of propagation used with outcome evaluations. This approach is designed for a discrete model of trust and more specifically binary ones. R. Guha et al. propose techniques for rounding the resulting values in the final matrix to bring the final results as either trust or distrust.

B. Predicting Trust

Most works on trust inference rely on matrix representation of the different values of trust that connects pairs of users (nodes). The calculation process idea, as introduced earlier, would be to explore these relationships for inferring an estimated trust value between two users. However, Haifeng Liu and al. [13] note that such process requires a high connectivity of the network to guarantee a path between any two given users and that it is generally not the case. This fact is also empathized through the studies of Alan Mislove and al. in [6] as well as in [3,8]. As a reaction towards this observation, Haifeng Liu et al. propose an alternative design for the prediction of a value of trust based on the behavior of users. This prediction seems more effective than the one presented in [16] since it is completely detached from the structure of the network graph.

1) Trust Based Prediction: The spare nature of social networks is a problem besides the fact that computing trust by propagation proceeds by multiplying vectors and matrices whose dimensions are extremely high which seems to be computationally expensive. In [16], prediction has overcome the fact that a complete network and explicit (annotated by all existing values of trust between pairs of users) is difficult to obtain, and so, it overcomes a critical situation unfavorable to any type of propagation. This is close to a reality witnessing that some users may not disclose their trust in others even in a centralized systems as well as in decentralized systems (decentralized communities, e.g.; the *Friend Of A Friend* ontology). Again, this type of prediction is therefore facing sparse nature of the connectivity and seems as an alternative when propagation comes short. However, it is based on learning from the portion of the global graph structure that can be covered as input for the supervised learning algorithm. Factors derived from connections such as performing relationship (assimilation of performances of users rated by the same tier, see the approximation of users in section III-A2) and judging relationship (assimilation between the values of common judgments on common users, see the ability to recommendation in section III-A2) are taken into account in determining relevant classification discriminators. In the case of a prediction approach, the previous factors would then be quantified and used for deciding the candidate value of trust

referring to a user trust boundary. For instance, take the covered graph portion of Figure 10 (From cooperative users who revealed their ratings toward others). The prediction indicators are computed as follows:

- Judging Relationship : which is used in this prediction case to approximate A and F's judging performances from A's point of view: $\frac{[|5-2|+...+|2-4|]}{n}$ (or another aggregation method)
- Performing Relationship : which is used in this prediction case to approximate F's performances from an exterior (public) point of view: $\frac{[|1-3|+...+|4-2|]}{m}$.

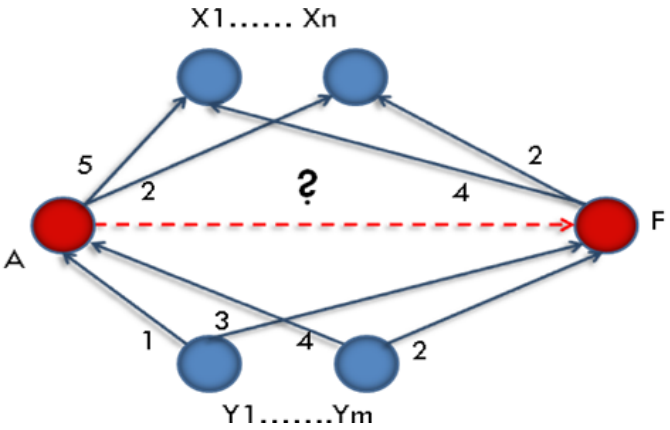

Fig. 10. Prediction based on the judging and performing relationships.

Related to the case studies in [16], this prediction is showed to be more effective then the propagation process in terms of performance and precision (Figures 11 and 12).

2) Interaction Based Prediction: The prediction approach introduced by Haifeng Liu et al. in [13] aims to increase the accuracy of the generated trust values by studying the evidence derived from significant users behaviors and interactions towards trust assignment. In other words, the authors here explore the graph in more depth by analyzing the different features qualified to be behind the assigned trust (see Figure 13). Haifeng Liu et al. have studied the case of Epinions, a general consumer review site that supports various types of interactions as well as a web of trust which can be used for training and evaluation. In Epinions, users can register for free and start writing subjective reviews about many different types of items (software, music, television show, hardware, office appliances, ...). A peculiar characteristic of Epinions is that users are paid according to how much a review is found useful (Income Share program). Also because of that, the attempts to game the systems are many and, as a possible fix, a trust system was put in place. Users can add other users to their "Web

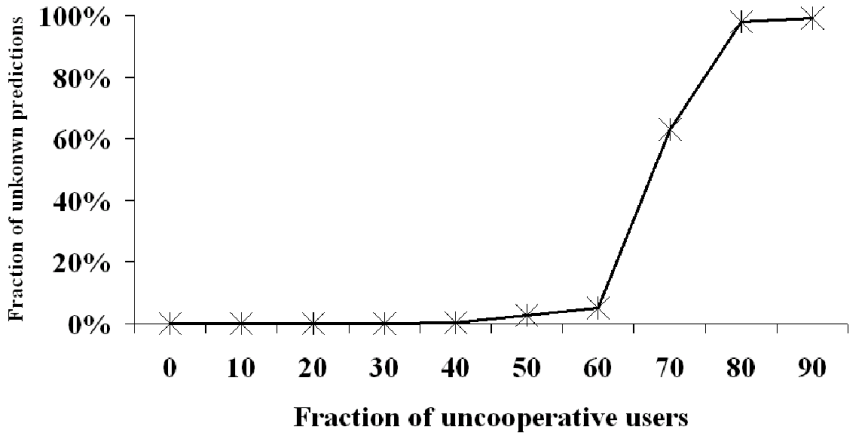

Fig. 11. Fraction of unknown predictions as a function of uncooperative users (users who are not willing to make their ratings available) as given in [16]

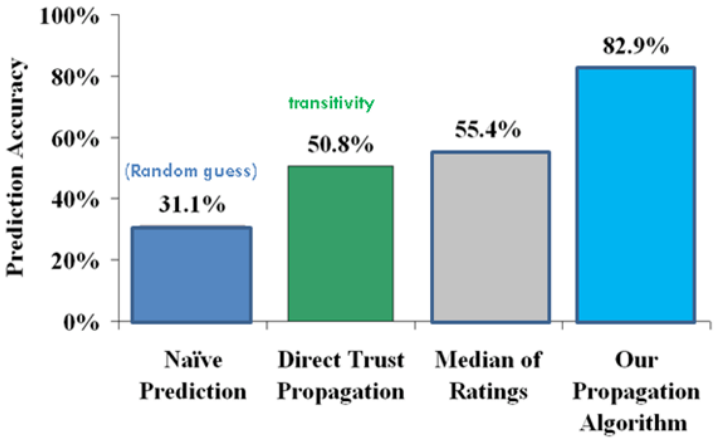

Fig. 12. Evaluation of the predictive accuracy of four algorithms as given in [16]

of Trust", i.e. "reviewers whose reviews and ratings they have consistently found to be valuable", and their "Block list", i.e. "authors whose reviews they find consistently offensive, inaccurate, or in general not valuable". Epinions is then a large collection of binary ratings and adopts a discrete model of trust. By binary we mean that each rating simply expresses whether an individual trusts another individual or not. The authors of [13] identify two types of taxonomies representing a user actions and possible interactions between pairs of the community:

1) The user actions taxonomy towards shared data such as reviews, posted comments, etc. Among these actions we mention: Number/frequency of posted reviews, num-

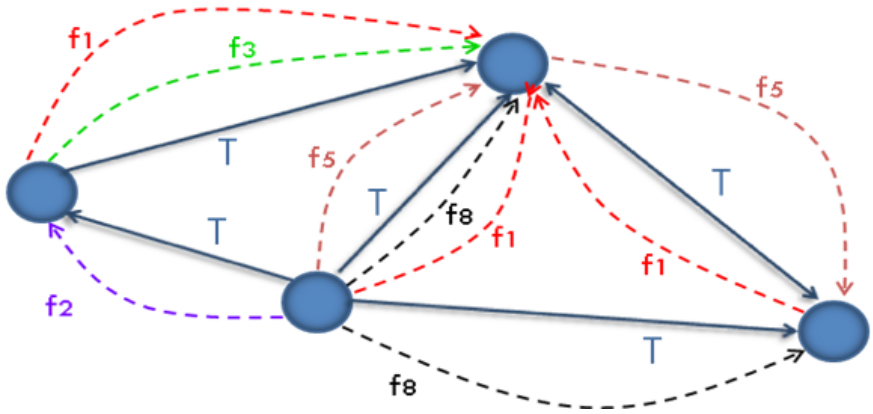

Fig. 13. Taking into account the different features behind pairs' trust relationships.

ber/frequency of ratings, Average length/number of comments given to reviews.

2) The pairs interactions taxonomy: enumerating the different possible interactions that could be held by two participants in Epinions.

Among these inter actions we mention:

- Interactions related to Writer-Rater (WR) Factors Connection: This group denotes the review set written by a given user u_i and rated by a second user u_j (as the absolute number of ratings with scores higher than 0.8 that are given to the writer by the rater).
- Interactions related to Writer Writer (WW) Factors Connection: applicable for the set of reviews written by a given user u_i and followed by u_j's reviews.
- Interactions related to Rater Rater (RR) Factors Connection: applicable for the set reviews rated by both u_i and u_j and where u_i's rating is before u_j 's rating.

In Epinions community, we can intuitively say that most likely trust is established after a certain level of interactions that happened between two users. Reason behind which a classification trough a supervised learning based on features like actions of a user and interactions between users was applied. As a result, interactions were showed to be most relevant discriminators behind the fact that a user assigns his trust for another.

IV. Our work on Trust Propagation

Previously, we introduced the different trust transitions and proposed to take into account weights for evaluating and approximating the users along the propagation path. We can adopt the propagation transitions in [7] (see Section III-A1) after launching the graph matrix. As

for transitivity, the factor F is the matrix B itself.
Iterations would be as follows:

$F \leftarrow B_0$ {Transitivity factor initiated with the initial Belief matrix B}
for $i \leftarrow 1$ to k **do**
{Suitably chosen k }
$B_i \leftarrow B_{i-1} \times F$
$B_0 \leftarrow B_0 + B_i$
end for

The factor for co-citation is $B^T.B$ and as opposed to transitivity, only one step co-citation may be generated. In other words, we only look after situations with strictly the same trust relation schemes as the one illustrated in Figure 4. Nevertheless, we noticed that applying the same steps of the preceding algorithm in case of co-citation may generate other values for existing trust information in the belief matrix. The addition of B_0 and B_i should be controlled in order to avoid replacing a non zero value of trust in the last B_0. Note that related to the experimental studies, transitivity and co-citation seem to be much more relevant then the two other transitions in one's decision on trust.

A. Propagation on a Recommendation Graph

In [7], the followed path in applying transitivity is a trust path, so that the result of a *distrust-distrust* path (*enemy of my enemy*) could be interpreted by some as a trust path leading to a friend, and some others may consider that the *enemy of my enemy* is a double distrusted enemy . Intuitively, following a path of recommendation seems to lead to a better results and could perfectly avoid the "enemy of my enemy" and "friend of my friend" questions. From our point of view, it would be interesting to explore the given web of trust and automatically generate the approximation factors to establish a superposed graph based on inferred links that would express the ability of recommendation that one could likely assign to another. In this way, we consider a propagation approach similar to the one introduced by R. Guha and al [7] following a path of recommendation links which ends with a functional trust link (the explicit initial trust) just as stated by Jøsang [11] (See Figure3). the same transitivity algorithm would now be as follows:

Similar to Quercia and al.'s idea in [16], we propose to build the matrix R by approximating

$F \leftarrow R$ {Transitivity factor initiated with the Recommendation matrix R}

for $i \leftarrow 1$ to $k-1$ **do**

{Suitably chosen k }

$B_i \leftarrow B_{i-1} \times R$

$B_0 \leftarrow B_0 + B_i$

end for

$B_k \leftarrow B_{k-1} \times T$ {In the last iteration, we multiply the result by the Graph's Trust matrix T}

$B_0 \leftarrow B_0 + B_k$

trust assignment behavior of every pair of users involved in the studied social network graph. We expect to get a better results with this extension; even if we do not exactly meet every detail of R.Guha et al. experiments, we try to compare the results with respect to the same new conditions that we adopt for this project.

B. Experimental Data

The Epinions Dataset is one of the most popular datasets for scientific communities interested on trust computing. TrustLet *(*$http://www.trustlet.org/wiki/Main_{P}age$*)*, for example, is a cooperative environment for the scientific research of trust metrics on social networks. It gives the opportunity to researchers to compare all proposed trust metrics on the same datasets. As our approach aims to reach best performances then achievements in [7], we worked on the same Epinion Dataset given for free download from the TrustLet website.

Epinions is a website where people can review products. Users can register for free and start writing subjective reviews about many different types of items (music, hardware, software, office appliances, television show, etc.). A peculiar characteristics of Epinions is that users are paid according to how much a review is found useful (Income Share program).

In this environment, the attempts to game the systems are many and, as a possible fix, a trust system was put in place. Users can add other users to their "Web of Trust", i.e. "reviewers whose reviews and ratings they have consistently found to be valuable", and their "Block list", i.e. "authors whose reviews they find consistently offensive, inaccurate, or in general not valuable". Our experimental Data Sample was picked from Epinions's web of trust files given at TrsutLet and described in the following.

- **user_rating** file : Trust is the mechanism by which the user makes a statement that he likes the content or the behavior of a particular user, and would like to see more of what he/she does in the site. Distrust is the opposite of the trust, in which the user says that he/she do want to see lesser of the operations performed by a particular user.
  Column Details:

  1) MY_ID, this stores Id of the member who is making the trust/distrust statement

  2) OTHER_ID, the other ID is the ID of the member being trusted/distrusted

  3) VALUE, equal to 1 for trust and -1 for distrust

  4) CREATION, it is the date on which the trust was made explicitly

- **mc** file: contains information on each article written by a user.
  Column Details:

  1) CONTENT_ID is an object ID for the article.

  2) AUTHOR_ID is the ID of the user who wrote the article

  3) SUBJECT_ID is the ID of the subject that the article is supposed to be about

- **rating** file: Ratings are quantified statements made by users regarding the quality of a content in the site. Ratings are the basis on which the contents are sorted and filtered.
  Column Details:

  1) OBJECT_ID is the ID of the object being rated. The only valid objects considered up to now are the reviews and essays (identified their content_idin a member_content table).

2) MEMBER_ID stores the id of the member (user) who is rating the object

3) RATING stores the 1-5 rating (1- Not helpful , 2 - Somewhat Helpful, 3 - Helpful 4 - Very Helpful 5- Most Helpful) of the considered object by a given member

4) STATUS indiquates the display status of the rating: 1 means the member has chosen not to show his rating of the object, and 0 means that the member does not mind showing his name beside the rating.

5) CREATION indicates the date on which the member first rated the object

6) LAST_MODIFIED is the latest date on which the member modified his rating of the object

7) TYPE is not used up to now. When Epinions will allow more than just content rating to be stored in this table, then this column would store the type of the object being rated.

8) VERTICAL_ID of the review.

The trust files can be viewed as a directed graph. The data they contain consists of 131 829 nodes and 841 372 edges, each labeled either trust or distrust. Of these labeled edges, almost 85% are labeled trust. We interpret trust to be the value +1 and distrust to be -1.

C. Experiments and Results

In our experiments, we performed only the transitivity and the co-citation as we consider they are the most relevant propagation mechanisms. We assigned the same weight for each of them e=(0,5; 0,5) and performed the five following schemes of propagation:

1) Trust + Distrust Transitivity (classic schema)
2) Recommendation Transitivity (based on users trust assignments approximation, we developed a graph of recommendation trust)
3) co-citation
4) Classic Transitivity and co-citation

5) Recommendation Transitivity and co-citation

1) The Random Sample: The necessary preprocessing of data and iterations were performed over MATLAB methods. We chose to evaluate the results applying the local rounding [7]: for each test vector (node) we calculate the trust and distrust threshold T and D. So over a resulting vector, we round the T biggest values as 1 (trust) and the D lowest values as -1 (distrust). Values that remain are rounded to zero.

At a first stage, we followed a random strategy to pick up 5% from total edges as a primal sample of the Epinions dataset, from which we obtain 18721 distinct participants. For the test procedure, we planed to hide 500 edges. The cross-validation method is the following. Given the trust graph, we mask a single trial edge (i, j) from the graph, and then ask each of the 5 schemes to guess whether i trusts j. At first, we were able to run the classic transitivity experience on 500 vectors. The multiplication by a trust matrix of (18721 $\times$ 18721) was possible. Unfortunately, the recommendation matrix that we got was very sparse given that the Sample were randomly chosen and that the pairs of users in the Samples do not have enough common trustees. Such matrix would effectively generate 500 almost-zero vectors. We thus reconsidered the possibility to build a recommendation matrix based not on trust approximation but on revues rankings approximation. This idea seems more interesting given that socially reviews are the largest portal by which users assess each other and readers build their opinions on writers. Scoring reviews could therefore be more relevant for evaluating recommendation relationships between pairs of users. Moreover, following this way we avoid the zero-matrix since the ranking revues data are much more abundant and the users activity over ranking is much more intense than over assessing trust. This explains the greater size of the file "rating" (683Mo) compared to that of trust information file "user_rating" (23.3 MB). This idea did not however work with a sample of 18721 node. The reason this time is the dimension of the relational PostgreSQL recommendation table we obtain. In fact, as we explained before, we run a Java program that performs the join for every possible pair of the 18721 sample nodes and returns the recommendation value if it exists.

2) The Most Active Peers Sample: as the recommendation table is effectively large, the join time the java method had to perform is of the order of 1 second per join (for 350 000 000 joins: 18721 $\times$ 18721). We therefore preferred to change strategy and redo the sampling. We opted for the idea of a sample less bulky but more relevant. So we proceeded as follows: From the whole graph we selected the most active trustors, i.e. those with more than 100

trustees. On the other hand, we selected the most frequent trustees, i.e. those who are trusted by more than 100 trustors. Then we retrieve the intersection of the two sets to get 1020 most active nodes in the community. This time, we noticed a rich users approximation recommendation matrix. We performed the cross validation process over 150 vectors to ask the prediction ability of each of the 5 schemes. Table 1 shows values for each experimental category.

Propagation mechanism	Local Rounding Precision
Transitivity(T+D)	19/150 (13%)
Transitivity Recom/Users	57/150 (38%)
co-citation	44/150 (29%)
Transitivity (T+D) and co-citation	60/150 (40%)
Transitivity Recom. and co-citation	100/150 (66%)

Table1. Prediction results. Here, $\mu_1 = 0.5$, $\mu_2 = 0.5$) and $K = 4$.

V. Additional refinements

A. *Propagation:*

Fixing arbitrary general weights for each transition would a generalizing point of view (as followed in [7]), which may not fit for all users. In a later stage, we propose to implement a way for calculating weights related to each user when estimating the trust he requires for another peer. Here, we are interested on weights for every introduced type of transition: transitivity, co-citation, trust coupling, transpose trust. Studying a user's tendencies by quantifying the importance of every type of relation in his past trust decisions is an interesting and possible track to follow. The period over which a user's behavior is studied is a parameter that can be configured. In order to reduce complexity, this parameter should be chosen with respect to the out-degree of a given user as a shorter period would be sufficient to generate a relevant result for most active users. We analyze the user's web of trust for the defined past period (e.g.: for last six days) counting the number of instances for each situation that could be around every past trust assignment in this period (number of co-citations, transitivity etc. leading to the given trustee). By aggregating the results, we can establish a rate for each type of propagation relatively to the total number of discovered instances.

B. Prediction:

The prediction approach aims to overcome the limit of propagation towards sparse connectivity of a graph. Factors such as *performing relationship* and *judging relationship* were proposed in [16] as significant discriminators for classifying pairs of users in the trust zone. As a future direction we intend to evaluate the possibility of considering them as weights reflecting the user's subjectivity in each transition formula when following a propagation approach for trust inference. The prediction based on the trust links seems interesting since the bridging of judgments and performance of two nodes may be a hidden information that both of them could not reach easily to evaluate the level of trust that one could assign to the other. Such information could be drawn based on trust relationships analysis that these two users hold with others in the community.

1) Interaction-Based Prediction Effectiveness: Interactions-based prediction requires a minimum threshold of interactions between A and B to satisfy the trust inference request. If we consider the case of Epinions community, a user who wants to know if he can trust another had logically not interacted enough with him to be able to figure out how trustworthy he would be. (For example, he/she read a single review for this author and does not have enough time to read more or see its activities but wants to know if he/she can trust him or not). In this case, the interactions-based prediction can not be established due to the lack of data required for classification. The prediction based on judging and performing relationships could lead with less input to a result. However, we may propose to perform a propagation of trust to the target node using the prediction of additional (implicit) trust links: if we can not find a leading path for the propagation due to the lack of explicit trust relationships, the idea of using two types of prediction on the graph seems interesting as it presents a way for concluding potential trust links between pairs which increases the density of the graph promoting a better trust propagation ground. Nevertheless, the proposed predictions are based on the discovery of a common behavior that could be behind the assessment of trust. For example, measuring the performing and judging relationships to place two users in the trust or distrust area referring to a fixed rate from a generalization of all users' decisions toward assigning or not the trust.

2) Evolutionary Prediction: The prediction would be much more robust and highly precise if it quantifies a discrimination boundary for each user and does not rely on a global behavior of users. By evolutionary, we thus mean a punctual and specific prediction for

every interacting peer in the network. This would be very efficient especially for a network where users' behaviors are highly convergent and difficult to approximate (e.g., in competitive communities where risk behind the actions is relatively high).

VI. Conclusion

The management of trust as well as access control in a *web of trust* are becoming key issues for many social web sites. The idea of estimating a direct trust rate between two actors in a social network is probably a fast and effective way. However, robust and accurate inference techniques for the calculation of such measures are necessary, given the number of constraints that could affect the accuracy of the result.

This report gives an overview of the existing work and approaches to the problem of trust inference and lists the methods followed for this aim. In a second part, we try to to generalize the previous work and describe the experiments we did on the Epinions dataset. These experiments enabled us evaluating the most effective methods of trust inference proposed in the literature and to test new extensions and refinements of existing approaches. We studied a new technique that involves relationships built through recommendation paths (judgments approximations) between users in a social network. Transitive propagation was experimented on this recommendation graph obtained from the Epinions dataset. Results shows that a recommendation could be a closer scheme to an user's subjectivity, which may come nearer to its own elements of decision making.

REFERENCES

[1] Karl Aberer, Zoran Despotovic, Wojciech Galuba, and Wolfgang Kellerer. The Complex Facets of Reputation and Trust. In *9th Fuzzy Days, International Conference on Computational Intelligence Fuzzy Logic Neural Networks Evolutionary Algorithms*, pages 283–294, 2006.

[2] Bader Ali, Wilfred Villegas, and Muthucumaru Maheswaran. A trust based approach for protecting user data in social networks. In *CASCON*, pages 288–293, 2007.

[3] James Caverlee, Ling Liu, and Steve Webb. Socialtrust: tamper-resilient trust establishment in online communities. In *JCDL*, pages 104–114, 2008.

[4] Guangzhu Chen, Zhishu Li, Zhihong Cheng, Zijiang Zhao, and Haifeng Yan. A fuzzy trust model for multi-agent system. In *ICNC (3)*, pages 444–448, 2005.

[5] Jennifer Golbeck. Trust on the world wide web: A survey. *Foundations and Trends in Web Science*, 1(2):131–197, 2006.

[6] Elizabeth Gray, Jean-Marc Seigneur, Yong Chen, and Christian Damsgaard Jensen. Trust propagation in small worlds. In *iTrust*, pages 239–254, 2003.

[7] R. Guha, Ravi Kumar, Prabhakar Raghavan, and Andrew Tomkins. Propagation of trust and distrust. In *WWW '04: Proceedings of the 13th international conference on World Wide Web*, pages 403–412, New York, NY, USA, 2004. ACM.

[8] Dan Hong and Vincent Y. Shen. Setting access permission through transitive relationship in web-based social networks. In *SWKM*, 2008.

[9] Audun Jøsang. Trust-Based Decision Making For Electronic Transactions. In *Proceedings of the Fourth Nordic Workshop on Secure Computer Systems (NORDSEC'99*, 1999.

[10] Audun Jøsang. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3):279–212, 2001.

[11] Audun Jøsang. Trust and Reputation Systems. In *FOSAD*, pages 209–245, 2007.

[12] Gabriella Kazai and Natasa Milic-Frayling. Trust, authority and popularity in social information retrieval. In *CIKM*, pages 1503–1504, 2008.

[13] Haifeng Liu, Ee-Peng Lim, Hady Wirawan Lauw, Minh-Tam Le, Aixin Sun, Jaideep Srivastava, and Young Ae Kim. Predicting trusts among users of online communities: an epinions case study. In *ACM Conference on Electronic Commerce*, pages 310–319, 2008.

[14] Samia Nefti, Farid Meziane, and Mohd Khairudin Kasiran. A fuzzy trust model for e-commerce. In *CEC*, pages 401–404, 2005.

[15] Jigar Patel, W. T. Luke Teacy, Nicholas R. Jennings, and Michael Luck. A probabilistic trust model for handling inaccurate reputation sources. In *iTrust*, pages 193–209, 2005.

[16] Daniele Quercia, Stephen Hailes, and Licia Capra. Lightweight distributed trust propagation. *Data Mining, IEEE International Conference on*, 0:282–291, 2007.

[17] Elizeu Santos-Neto, Matei Ripeanu, and Adriana Iamnitchi. Tracking user attention in collaborative tagging communities. In *CAMA*, pages 11–18, 2007.

[18] Cai-Nicolas Ziegler and Georg Lausen. Propagation models for trust and distrust in social networks. *Information Systems Frontiers*, 7(4-5):337–358, 2005.