Trust and Reputation Model for Various Online Communities

Lenuta Alboaie[1], Mircea-F. Vaida[2]

[1] Computer Science Department, Alexandru Ioan Cuza University of Iasi, Romania,
16,Berthelot, Iasi, Romania,
adria@infoiasi.ro

[2] Communication Department, Technical University Of Cluj-Napoca,
26-28, Gh. Baritiu Street, Cluj-Napoca, Romania,
mircea.vaida@com.utcluj.ro, corresponding author

Abstract: In World Wide Web there are many online communities with a huge number of users and a great amount of data which are continuously increasing. In this context it is important for users to interact with resources and other users according to their preferences. On this direction of information filtering domain our work is oriented to trust based filtering. We have developed a model formed by three interconnected components: trust component which allows computation of trust levels among users which are not directly connected, a component which computes reputation of entities in the system, and a recommendation component. Several sets of tests of our model have been performed and we have the possibility to integrate it in various online communities.

Keywords: online community, social trust, local trust metric, reputation, recommendations

1. Introduction

The existing technologies have led to an increasing interaction between people who do not know each other. In this case, online interactions replace human interactions. An important goal of our article is to improve these interactions based on two important concepts: social trust and reputation.

Trust and reputation are two interrelated concepts. We can find trust at personal level. Reputation expresses an opinion resulting from collective opinions of community members. This type of evaluation may lead to risks such as penalty of innovative and minority ideas, problem described in (Tocqueville 1840), (Massa, Avesani 2007) as “tyranny of the majority”. Naturally, the opinions of minority groups matter and should be seen as opportunities. But if minority groups obtain a full priority, it is obtained the other extreme, the so-called phenomenon of "echo chamber". In this case, as shown in (Sunstein 2009) will result a fragmentation of society into micro-groups that tend to sustain extremely their opinions.

Nowadays, there are many online communities (community for sharing resources, social networks, scientific communities, etc.), that store a great amount of data which are continuously increasing. Anyone can publish any kind of resources: a diary published within a blog, a track that a user wants to make public, etc.

In this context in which users have to interact with other users about whom they don’t have any previous information, and in which the overloaded information phenomenon brings a major impact, this paper comes up with a solution to improve the interactions among users and resources management.

The proposed trust and reputation model assures that users experience resulted from the previous interactions are used to establish user-user and user-resource evaluation levels.

Therefore, the purpose of the paper is to find a solution based on trust and reputation to provide users from online communities a balanced combination of personal vision with a global perspective on the community that will provide the opportunity to interact with users and resources that are relevant to them.

Section 2 presents the trust and reputation concept and the main proposals that exist in the scientific literature. Section 3 presents our trust and reputation model based on a set of published results (Alboaie 2008), (Alboaie, Barbu 2008), (Alboaie, Vaida 2010).

Section 4 provides details about our model architecture and the results obtained from several tests are presented. A comparison with the most relevant local trust metric, Mole Trust has been performed. Section 5 will contain the conclusions and the future work.

2. Related Work

In each of the areas in which trust plays an important role, e.g. sociology, psychology, political science, economics, philosophy and computer science, were given various definitions of the trust concept.

The definition of trust concept accepted by great majority of the authors is presented in (Gambetta 1990): "Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends". This action is in online communities an evaluation, an opinion that someone expresses regarding someone else and is quantified by numerical values.

The concept of social trust is associated with four properties (Golbeck 2005b): *transitivity*, *composability*, *personalization*, *asymmetry*.

These properties make it possible to calculate trust. Trust is not perfectly transitive in the mathematical sense, but trust can be transmitted between entities.

The *composability* property specifies how the associated ratings of trust are propagated between entities which are not directly connected.

The third property is the personalization of trust, this means that on the entity C, A and B may have different opinions. Another property of trust is the asymmetry and means that if A trusts B, B may not have the same trust level in A. We are dealing with so-called *one-way trust* (Hardin 2002). In essence, trust is represented by a user judgment concerning other user, sometimes carried out directly and explicitly, sometimes indirectly through assessment of various actions taken by the same user.

Trust is calculated in a so-called *trust network*. Trust network is a graph obtained by aggregating users' evaluations. These evaluations can be quantified, so we have different levels of trust that can be established between users. In such a trust network can run a so-called *trust metric* which is actually an algorithm that receives input information from the network and calculates various values of trust among users (Massa 2006). In the literature it is used the trust metric notion, where metric does not signify as the mathematical concept of metric, being a distance function.

A first trust metric was developed in (Levien 2003) within the Advogato system where the metric was used to determine how members can trust among community members.

In this paper we use the notion of trust metric or algorithm for measuring trust in the sense described above.

Trust metrics are divided into *local trust metrics* and *global trust metrics*. Global metrics take into account all existing nodes and links of trust. A global value is assigned to an agent based on all network information. Many global trust metrics such as (Sepander et al 2003), (Guha 2003) were inspired from the PageRank algorithm (Page et al 1998) that calculates the reputation of Web pages.

Local trust metrics take into account personal interactions. A local trust metric calculates trust from subjective opinion of an entity. Thus, the trust value associated to an entity varies for each existing agent in the system.

For the concept of reputation we stopped on the two definitions we encounter in Merriam-Webster's dictionary and in the Compact Oxford Dictionary:

Definition1: overall quality or character as seen or judged by people in general.

Definition2: the beliefs or opinions that are generally held about someone or something

In (Mui et al 2002) is identified a property which characterizes the relationship between trust and reputation: *reciprocity*. The reciprocity is defined as the reciprocal exchange of assessment (favourable or not). Decrease any of these automatically conduct to the reverse effect.

In (Massa, Avesani 2007) is clearly illustrated the difference between a global and a local metric when the entities over which there are divergent points of view are highlighted. It is natural that users have different views on a user, but this does not mean that one opinion is correct and the other not. Actually must be considered that they just disagree. With a global trust metric the controversial users' aspect cannot be surprised.

In literature we find very few models of local trust metric (Zieglar, Lausen 2004), (Golbeck

2005b), (Massa, Avesani 2006) or a proposed trust metric (Zhili et al 2009) which extends the metric from (Massa, Avesani 2006).

In majority of cases the computing models are based on the global trust or reputation, and in (Josang 2007) was made a classification of reputation systems and used calculation methods: calculation of the ratings sum (e.g., eBay), averaging ratings (e.g. Amazon, Epinions) using Bayesian systems (e.g. systems proposed at the theoretical level (Nurmi 2006), (Mui et al 2002)), using discrete trust models (e.g. the model proposed in (Rahman, Hailes 2000)), using a fuzzy model (e.g. systems proposed in (Sabater, Sierra 2002)), using flow models (e.g., Google Page Rank (Page et al 1998), Advogado (Levien 2003) Appleseed (Ziegler, Lausen 2004)).

One of the novelties carry out in this paper is a model that provides to users, both a local personalized vision of the system provided by our local trust metric, and a global vision given by a mechanism that compute the reputation.

3. Trust and Reputation Proposed Model

In this section will be described the proposed trust and reputation model, named StarTrust. StarTrust is based on experiments and tests realized with a previous model, StarWorth (Alboaie 2008), (Alboaie, Barbu 2008), (Alboaie, Vaida 2010). StarTrust contains in addition a mechanism for trust propagation that take into account the untrust factor that may exist between two users. StarTrust will contain a reputation component that provides to systems that integrates our model, a balance between two factors "echo chamber" and "tyranny of majority." The StarTrust model is made up of three main elements:

– Trust component,

– Resource recommendation component,

– Reputation component.

We will consider the following terms:

– Users - are members of an online community.

– Resources - their definition is made accordingly to the definition given by (T. Berners-Lee 1998).

– Worth - is a measure that signifies an evaluation accorded by a user to another user or resource. Also, the worth can be obtained (quantized) indirectly as we will see in the following paragraphs. In our system we consider five evaluation levels with the following semantic:

Table 1. Levels of evaluations with their significance

Level1	Level2	Level3	Level4	Level5
(0,1]	(1,2]	(2,3]	(3,4]	(4,5]
useless/spam	poor	worth attention	good	exceptional

We note the upper limit with *MaxWorth*, where *MaxWorth* = 5 in our experiments.

Trust component

The purpose of this component is to provide users from an online community a personalized vision of the system. We considered a set of constructions that will be used in the following sections and which have the following associated semantics. In fact, these constructions can be mathematically considered as functions or, from the implementation point of view, they are considered associative tables:

– Explicit worth of a user: $WE\_UU(user_i,user_j)$ – explicit worth, represents the rating for $user_j$, and the rating is given manually by the $user_i$ to $user_j$.

– Implicit (deducted) worth of a user: $WE\_UU(user_i,user_j)$ – measures how close are of both preferences.

(The preference can be considered the accepting degree of a point of view).

We consider the function $WE(user_i,user_j)$ for each pair of $(user_i,user_j)$ that contains the explicit and implicit evaluations:

$$WU(U_i,U_j) = \\ = \begin{cases} WE\_UU(U_i,U_j), \text{ if } U_i \text{ explicitly eval. } U_j \\ WI\_UU(U_i,U_j), \quad \text{otherwise} \end{cases} \quad (1)$$

We will define the manner of computation of the implicit values introduced above.

Let us consider two users U_i, U_j. The value of $WI\_UU(U_i,U_j)$ indicates the deducted worth based on explicit evaluations made by users to each other. Let consider the users U_i, from whom we have ratings to $\{U_i^1,...,U_i^k\}$. Also, we consider having explicit ratings from U_i^l to U_j, $l \leq k$ so we have defined $WE\_UU(U_i^l,U_j)$ (see Figure 1).

We have $WU(U_i,U_i^l) = WE\_UU(U_i,U_i^l)$ if there exists an explicit evaluation from U_i to U_i^l, otherwise we consider an implicit evaluation from U_i to U_i^l.

Our model in this phase only surprise the trust that user U_i will accord to U_i^l that will made a correct evaluation of U_j from his point of view.

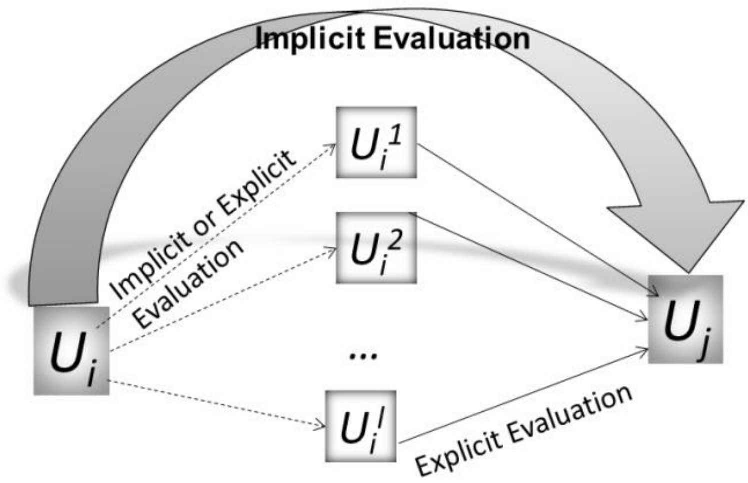

Figure 1. Implicit user-user evaluation computation

In order to compute WI_UU we must to compute the value of the weight corresponding with the explicit ratings. We denote this weight with $P_E(U_i^l,U_j)$. The weight represents (from the point of view of U_i) an explicit rating, in our case the rating weight given by U_i^l to U_j and it is computed as follows:

$$P_E(U_i^l,U_j) = \frac{WU(U_i,U_i^l)}{MaxWorth} \quad (2)$$

We compute the implicit rating that user U_i provided to U_j as:

$$WI\_UU(U_i,U_j) = \frac{1}{k} * \sum_{l=1}^{k} P_E(U_i^l,U_j) * WE(U_i^l,U_j) \quad (3)$$

where, $1 \leq l \leq k$, k is the number of the users that were explicitly evaluate by U_i. From (2) and (3) we obtain the implicit reputation computing formula that we used in tests and experiments realized in our previous works:

$$WI\_UU(U_i,U_j) = \frac{\sum_{l=1}^{k} WU(U_i,U_i^l) * WE(U_i^l,U_j)}{k * MaxWorth} \quad (4)$$

But the model does not surprise the fact that it is possible that U_i^l don't realize a correct evaluation from U_i point of view. For a better understanding of the necessity to surprise such an aspect will begin to examine a particular case and we consider:

- three users U_1, U_2, U_3
- $WE\_UU(U_1,U_2)$ is the trust value given in an explicit mode by user U_1 to U_2, $WE\_UU(U_2,U_3)$ is the trust value given in an explicit mode by user U_2 to U_3.

We want to analyze the following (see Figure 2):

- how to obtain the trust value $WI\_UU(U_1,U_3)$ (that represents the trust value given in implicit mode of U_1 to U_3, that the system will compute)
- how relevant is that value for U_1

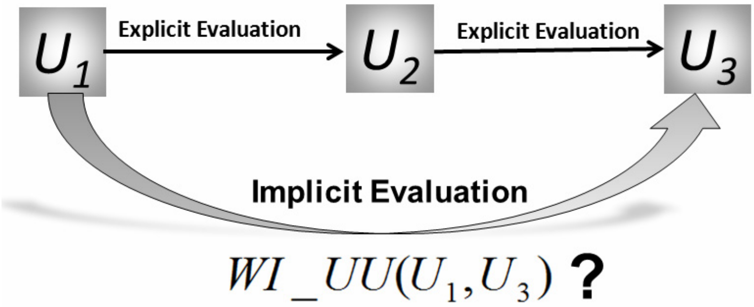

Figure 2. Implicit evaluation between two entities

Considering relation (4) the value $WI\_UU(U_1,U_3)$ will be computed thus:

$$WI\_UU(U_1,U_3) = \frac{WE\_UU(U_1,U_2)}{1*MaxWorth}*WE\_UU(U_2,U_3)$$

Ratio $\frac{WE\_UU(U_1,U_2)}{1*MaxWorth}$ represents the probability that U_2 will make a correct evaluation of U_3 from the point of view of U_1. We mention that any evaluations are correct, that provides the existence of local trust metrics.

User U_1 does not know that U_2 will make a correct evaluation, and thus to surprise such a possibility of an incorrect evaluation the general relation to compute $WI\_UU(U_1,U_3)$ must be as follows:

$$WI\_UU(U_1,U_3) = \frac{WE\_UU(U_1,U_2)}{1*MaxWorth}*$$
$$*WE\_UU(U_2,U_3)+(1-\frac{WE\_UU(U_1,U_2)}{1*MaxWorth})*P_{TC}$$

Where: P_{TC} is named *trust control parameter*, representing a probable implicit trust that is accorded to any user in system.

The expression $1-\frac{WE\_UU(U_1,U_2)}{1*MaxWorth}$ represents the probability that U_2 to have no right in evaluation of U_3 from the point of view of U_1.

If $WE\_UU(U_1,U_2)$ has a big value (U_1 has a maximum trust in U_2) the value of the expression $(1-\frac{WE\_UU(U_1,U_2)}{1*MaxWorth})*P_{TC}$ will be close to 0 and the relation will be simplified to formula (4).

We consider users U_i and U_j from a community. We consider $\{U_i^1,...,U_i^k\}$ the set of users to whom there are explicit or implicit ratings from user U_i. We also consider that exist explicit ratings from U_i^l to U_j, $l \le k$.

The general formula to compute implicit trust is (5):

$$WI\_UU(U_i,U_j) = \frac{\sum_{l=1}^{k} WU(U_i,U_i^l)*WE(U_i^l,U_j)}{k*MaxWorth}$$
$$+(1-\frac{\sum_{l=1}^{k} WU(U_i,U_i^l)}{k*MaxWorth})*P_{TC}(U_i,U_j)$$

We used the notation $P_{TC}(U_i,U_j)$ to specify that P_{TC} is not absolute a constant, the value may vary depending on the user that realize the evaluation and the user that receive the evaluation.

Therefore we have defined a general local trust metric that may be adapted to any type of community by means of the values that may be associated to parameter P_{TC}. The experiments from this paper will consider values for parameter P_{TC}=0, and also different of 0.

If P_{TC} is 0, than the trust accorded to far nodes is smaller as the distance to the source node is bigger.

Depending on the community were we integrating StarTrust, we may choose more values of P_{TC} parameter:

– in a close community (such as a scientific community) the value can be considered 0. Considering this value, all ratings from users who are at large distances in the graph will be increasingly smaller. In this way is minimized the influence of users who are not very close to the source node.

- in a community such as an online community where it is not possible to define the profile of the users, the value for P_{TC} could be considered as the reputation of the user.
- in other communities we may consider P_{TC} having as value the media value of the given explicit evaluations or the media of first 10% of good evaluations, so depending of the type of the community we may consider specific values for this factor.

How the ratings are lower, the member $1-\frac{\sum_{l=1}^{k} WU(U_i, U_i^l)}{k * MaxWorth}$ will be close to 1, so that the importance of P_{TC} is essential (in this case the distance between users doesn't matter).

We consider as follows the pseudo code for local trust metric from StarTrust. We have the following notations:

- *sourceUser* – is user for which is calculated the vision over community;
- *WU* – contains the evaluation from trust network in community at a given time
- *WE* – contains the explicit evaluations from *WU*
- *sinkUsers* – are users that received evaluations from *sourceUser*

Input: *sourceUser, WE, WU*
Output: *WU, sinkUsers*
Step 1. add in *sinkUsers* all nodes accessible from *sourceUser*
Step 2. **do** *savedWU* = currentTrustNetwork;
 Step 3. Foreach *U* în *sinkUsers*
 Step 4. Find $\{U_i^1,...,U_i^k\}$ satisfying the following conditions: (there is an edge between *sourceUser* and each U_i^k in WU) and (there is an edge between each U_i^k and U in WE)
 Step 5. Calculate implicit trust value between *sourceUser* and *U*using (5):

$$WU(sourceUser, U) = \frac{\sum_{l=1}^{k} savedWU(sourceUser, U_i^l) * WE(U_i^l, U)}{k * MaxWorth} + (1-\frac{\sum_{l=1}^{k} savedWU(sourceUser, U_i^l)}{k * MaxWorth}) * P_{TC}(sourceUser, U)$$

/* Update or insert an edge between *sourceUser* and *U* with capacity computed at Step 5 in *WU* */
 while (*savedWU* != *WU*)

Algorithm 1. StarTrust – local trust metric

The stop condition ($savedWU \mathrel{!=} WU$) is materialized in implementation through election of a ε value, so that two matrix *savedWU*, *WU* are in different relationship if there exists indices *i* and *j* so that $(WU[i, j] - savedWU\ [i, j]) > \varepsilon$.

Resource recommendation component

In the context of traditional recommendation systems, users give ratings to resources and based on these ratings the system will make recommendations. The standard mechanism used in recommendation systems (e.g. Person Correlation) causes cases in which a recommendation system does not provide satisfactory results, and we mention (Massa, Avesani 2006): extending the period of real integration of new users or promotion of a new resource added to the system is realized for a long period.

The goal of the proposal component is to build a flexible way to manage resources in a personalized manner. In order to achieve this we shall consider a mechanism that is based on the trust relation among users, which already have evaluated other resources.

We shall consider the following constructions:

- *WE_UR*(*user$_i$*,*resource$_j$*) - represents the explicit evaluation given by *user$_i$* to *resource$_j$*.
- *WI_UR*(*user$_i$*,*resource$_j$*) - represents the implicit evaluation value, computed by system and that *user$_i$* associate to *resource$_j$*

Let us consider $WR(user, resource)$ function, for every pair (*user*, *resource*):

$$WR(U_i, R_j) = \begin{cases} WE\_UR(U_i, R_j), \text{ if } U_i \text{ explicitly eval. } R_j \\ WI\_UR(U_i, R_j), \quad \text{otherwise} \end{cases} \quad (6)$$

Using the same reasoning presented for computing trust between users, we obtained the implicit rating from user U_i to R_j **(7):**

$$WI\_UR(U_i, R_j) = \frac{\sum_{l=1}^{k} WU(U_i, U_i^l) * WE\_UR(U_i^l, R_j)}{k * MaxWorth}$$

Using this component a system can provide a hierarchical personalized ranking of resources based on user's vision, so we have a recommendation based resource mechanism that uses both the ratings given by users to resources and the ratings given among the users.

Reputation component

As presented in Section 2 the concepts of trust and reputation are closely linked. Reputation is a value that signifies the image of a community concerning a user. For our system we consider a general formula for calculating the reputation, we justify the choices and we show that it can be customized for various online communities that may exist.

We consider a user U_i. We note with $N_l^i = \{Ev_l^1, Ev_l^2, ..., Ev_l^k\}$ the set of ratings that user U_i have received in the interval given by level $l, 1 \le l \le MaxWorth$, $MaxWorth$=5.

We note with $\left|N_l^i\right|$ the cardinal of N_l^i that represents the number of ratings that a user received from the given interval. We consider for a user the general reputation formula so:

$$\text{Rep}(U_i) = \sum_{l=1}^{MaxWorth} \frac{\left|N_l^i\right|}{\sum_{j=1}^{MaxWorth} P_{LW}^j * \left|N_j^i\right|} * P_{RC}^l \qquad \textbf{(8)}$$

where: P_{RC}^l is the reputation control parameter, P_{LW}^j is the level weight parameter

Choosing justifications:

Intuitively, the global reputation of a user should take into account the actual received ratings and the number of ratings he received for each rating level. In the calculation of reputation, the ratio $\frac{\left|N_l^i\right|}{\sum_{j=1}^{MaxWorth}\left|N_j^i\right|}$ represents the importance of the number of ratings that a user was evaluated in an interval. Intuitively, we consider that P_{LW}^j is 1. This factor will help us to adjust the importance of each evaluation level to compute the reputation.

The factor P_{RC}^l goal is to adapt the computation of reputation value to the community profile.

We consider different possibilities to select this factor. In previous studies it was imposed the restriction that the value of reputation to be in the interval [0, MaxWorth]. A method to provide this thing is to choose the factor P_{RC}^l to have a value in the specified interval of level *l*. So if we have the interval [m, M], $0 \le m < MaxWorth, 1 \le M \le MaxWorth; m, M \in Z$ must respect the condition: $m \le P_{RC}^l \le M$. In this case is easy to demonstrate that the computed reputation will be in the interval [0, *MaxWorth*].

We present a possible choosing values for parameters for the adjusting the reputation

If P_{RC}^l has as value the ratings media on a given interval *l*, the formula to compute reputation is reduced to determine the arithmetical media, this being a mechanism consider by many functional real systems (e.g. eBay). If we have a close community where we are able to give a certain trust level (as example a scientific community), than we may consider $P_{RC}^l = \max N_l^i$. If we have an open community where the community members are able to easy change the identity and it is not possible to establish a general profile of the community users, we may consider $P_{RC}^l = \min N_l^i$.

This parameterization to compute reputation presents an aspect that is not considered by the majority of the existed literature models. Thus, the adaptation computing mechanism of reputation can be modeled depending on the community type where is used.

For the next studies we will eliminate these restrictions and we will consider that only trust, which is subjective, must be integrated in such an interval. Reputation is better to do not be limited to an interval. Thus, the reputation will reflect a real unlimited value of the user. We presented that reputation can be used in the relation to compute the trust, and for that we will provide a corresponding scaling.

StarTrust Implementation

StarTrust was developed as a model that once integrated in a community is able to provide the following services: trust relations among users provided by trust component, users reputation provided by reputation component and a service that is able to recommend resources depending on preferences expressed by users using the resource recommendation component.

The model implementation was realized by implementing the three components with their interactions.

In the first step were considered formulas (1)-(5). In this step the aim was to obtain user trust vectors. We consider a set of users $\{U_1,...U_n\}$. To each user from the system is associated a trust vector. Also we consider the matrix R that contains the ratings:

$$R(i, j) = \text{rating given by } U_i \text{ to } U_j, \forall i,j \in [1,n]$$

The ratings from R are explicit or implicit ratings obtained by relations (1)-(5).

We consider the following algorithm that computes the elements of R matrix. We consider the constructions:

– RE – explicit rating matrix;

– R – current ratings matrix of the system;

Input: RE

Output:R

Step 1. R=RE

Step 2. Insert the rating R(i,j) = *MaxWorth* for $\forall i = j$, $1 \le i \le n$, $1 \le j \le n$

Step 3. For each i, $1 \le i \le n$

execute the **Algorithm 1** using:

- i as *sourceUser*
- RE *as WE*
- R as *WU*

Algorithm 2. Algorithm of trust propagation in whole community

The second step in the implementation process of the ratings mechanism will consider formulas (6)-(7). In this step the aim is to obtain relevant resources concerning a user point of view. So were computed the vectors that will contain the given ratings by a certain resource from system users. These ratings represent actually the interest level that a user has for a resource.

We consider:

– $\{U_1,...U_n\}$ the users set

– $\{R_1,...R_m\}$ the resources set

The next algorithm will compute the elements of RR matrix that contains evaluations for resources in [0, *MaxWorth*] range:

Step 1. Insert the explicit ratings in *RR*

Step 2. For each i, $1 \le i \le n$

Step 3. For each j, $1 \le j \le m$

Find $\{U_i^k,...,U_i^k\}$ satisfying the following conditions:

User U_i evaluates each of these users

There exists an explicit evaluation from users $U_i^k,...,U_i^k$ to R_j

We compute the value $RR(i, j)$ using (7)

Algorithm 3. Resource associate ratings compute algorithm

Remark: Obviously if does exist no user U_i^j, $1 \le j \le m$ that evaluated resource R_j than $RR(i, R_j) = 0$. Finally we obtain the value of *RR* that represents the implicit and explicit evaluations that users associated to the system resources at a given moment.

With these values the system can recommend a hierarchy relevant resources for each user.

4. Experiments with StarTrust

To test the local trust algorithm we need the communities for this testing. In the specialized literature the local trust metric tests proposed have been accomplished on the dates from Epinions in (Massa, Avesani 2007) or in (Zieglar, Lausen 2004) have been created their own dates for tests. In this work we chose to analyze and to generate data that are useful in obtaining conclusions on the system, without introducing factors which would not be necessary or could even impede a correct analysis. The generation of the test’s data is made by using a generator called DataTestGenerator (M. Breaban, 2009), which can be customized to generate different cathegories of explicit evaluations which mirror evaluations that can also be found within the online communities.

Tests and results

Use Case. We want to study trust propagation and how works StarTrust in a community of 15 users that have 20 resources.

Remarks: This small number of users and resources was chosen considering graphic limitations for visualization.

Using the data generator we obtained the explicit user-user evaluations:

0.00 0.00 0.00 0.00 0.00 4.00 0.00 3.00 0.00 0.00 0.00 0.00 4.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 4.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 1.00
0.00 0.00 3.00 0.00 0.00 0.00 0.00 0.00 3.00 0.00 0.00 0.00 1.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 4.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 2.00 0.00
0.00 0.00 4.00 3.00 0.00 0.00 0.00 0.00 3.00 0.00 0.00 0.00 0.00 0.00 0.00 3.00 0.00 0.00 0.00 0.00
0.00 0.00 0.00 0.00 0.00 4.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 3.00 0.00 0.00 3.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 2.00
0.00 0.00 0.00 0.00 3.00 0.00 3.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 4.00 1.00
0.00 0.00 0.00 0.00 0.00 4.00 3.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 3.00 0.00 1.00 2.00 0.00
0.00 0.00 0.00 0.00 0.00 0.00 0.00 3.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 4.00 0.00 0.00 3.00 3.00 0.00 0.00 0.00 0.00 0.00 2.00 0.00 0.00 1.00 2.00 0.00 0.00 0.00 0.00
0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 3.00 0.00 0.00 0.00 1.00 0.00 0.00 0.00 1.00 0.00
4.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 1.00
3.00 0.00 3.00 0.00 0.00 4.00 4.00 0.00 3.00 3.00 0.00 0.00 2.00 0.00 0.00 0.00 4.00 1.00 0.00 4.00

If we consider that the community is a new one, composed for example with students that will not easily change the identity, we can consider P_{TC} =2.5. Using trust computing component from StarTrust we obtain the implicit evaluations.

Also, using trust recommendation component we obtain the matrix that contains the explicit generated ratings for resources and implicit computed ratings for resources:

0.00 0.00 0.00 0.00 3.00 4.00 3.00 3.00 0.00 0.00 0.00 0.00 4.00 0.00 0.00 0.00 0.00 0.00 4.00 1.00
0.00 0.00 2.90 0.00 0.00 0.00 0.00 0.00 4.00 0.00 0.00 0.00 1.30 0.00 0.00 0.00 0.00 0.00 0.00 1.00
0.00 0.00 3.00 0.00 0.00 2.90 0.00 0.00 3.00 0.00 0.00 0.00 1.00 0.00 0.00 0.00 0.00 0.00 0.00 2.10
0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 4.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 2.00 0.00
0.00 0.00 0.00 0.00 0.00 3.40 2.80 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 2.80 0.00 1.60 2.00 0.00
0.00 0.00 4.00 3.00 0.00 0.00 0.00 0.00 3.00 0.00 0.00 0.00 0.00 0.00 0.00 3.00 0.00 0.00 0.00 0.00
0.00 0.00 0.00 0.00 0.00 4.00 0.00 3.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 3.00 0.00 0.00 3.00 2.90 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 2.90 0.00 1.30 2.10 2.00
0.00 0.00 2.90 0.00 3.00 0.00 3.00 0.00 2.90 0.00 0.00 0.00 1.30 0.00 0.00 0.00 0.00 0.00 4.00 1.00
0.00 0.00 0.00 0.00 0.00 4.00 3.00 0.00 0.00 0.00 2.70 0.00 0.00 0.00 1.90 3.00 0.00 1.00 2.00 0.00
2.80 0.00 0.00 0.00 0.00 0.00 0.00 3.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 2.20
0.00 4.00 0.00 0.00 3.00 3.00 0.00 0.00 0.00 0.00 3.00 2.00 0.00 0.00 1.00 2.00 0.00 0.00 1.00 0.00
0.00 2.80 0.00 0.00 2.60 2.60 0.00 0.00 0.00 0.00 3.00 2.40 0.00 0.00 1.00 2.40 0.00 0.00 1.00 0.00
4.00 0.00 0.00 0.00 2.90 0.00 2.90 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 3.70 1.00
3.00 2.80 3.00 0.00 2.60 4.00 4.00 2.80 3.00 3.00 0.00 2.40 2.00 0.00 2.20 2.40 4.00 1.00 0.00 4.00

From this matrix we extract hierarchy of relevant resources for each user.

Table 2. Hierarchy resources vision of every member of community

User Identification	Resources sorted by relevance
User Id=1	6 13 19 5 7 8 20
User Id=2	9 3 13 20
User Id=3	3 9 6 20 13
User Id=4	9 19
User Id=5	6 7 16 19 18
User Id=6	3 4 9 16
User Id=7	6 8
User Id=8	3 6 7 16 19 20 18
User Id=9	19 5 7 3 9 13 20
User Id=10	6 7 16 11 19 15 18
User Id=11	8 1 20
User Id=12	2 5 6 11 12 16 15 19
User Id=13	11 2 5 6 12 16 15 19
User Id=14	1 19 5 7 20
User Id=15	6 7 17 20 1 3 9 10 2 8 5 12 16 15 13 18

We notice that in spite that the user with ID=2 (U_2) has evaluated in explicit mode only one resource (resource with ID=9 - R_9 with a rating with value 4 depicted in matrix with user-user explicit evaluations), the system will be able to suggest a resource hierarchy suitable with his preferences, considering trust evaluations that he associate to other users.

We analyze the recommendations provided by the system to user U_2. The resource R_3 was recommended because user U_2 evaluated U_3 with a 4 rating and this user have already an evaluation for resource R_3, therefore StarTrust uses this experience to recommend new resources.

We remark that in Table 2 we have the entire resource hierarchy accessible for users, and from the matrix of explicit and implicit user-resource evaluations, we may identify the computed ratings for each resource and easily we may establish a threshold of evaluations, that will give the possibility to obtain the two sets of resources recommended or un-recommended.

If for our example we use a threshold with value 2 than from matrix of explicit and implicit user-resource evaluations we may observe that the recommended resources for user U_2 will be R_9 and R_3 in this order. Thus the system ensures that the user will not have to interact with irrelevant resources for him and his actions in the community can be safer and more efficient. The user also, has its own image of the users from the system.

Using reputation component from StarTrust we obtain the following results:

In StarTrust, we consider that to eliminate the graph circuits will affect the results accuracy. We consider that the MoleTrust argument regarding computing time reduction will affect the trust propagation. In StarTrust the computing algorithm is equivalent with solving a linear system of equations (Alboaie 2009). To analyze the effect of the results affected by eliminating circuits we consider the following example: user A may be interested that B and C are evaluated in a

Table 3. Reputation values for community members

User Id	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Reputation value	3.00	0.00	3.31	0.00	5.00	0.00	0.00	3.12	3.53	3.05	5.00	1.93	2.85	1.38	0.00

As we specified previously, we considered a student community and for such a profile we may consider the following control parameters associated to reputation compute value:

– reputation control parameter P_{RC}^{l} will take as value the media of ratings for level l, where $N_l^i = \{Ev_l^1, Ev_l^2, ..., Ev_l^k\}$ is the set of ratings that user U_i received in the interval specified by level *l*, $1 \le l \le MaxWorth$, *MaxWorth*=5

– for level importance control parameter P_{LW}^{j} we considered value 1 for levels.

Therefore, using the functionality offered by all 3 components, StarTrust will provide in the context of a huge amount of data and a huge number of users, an interaction with resources and relevant users for each user, or for new users a rapid integration in the system.

Comparison with MoleTrust

The proposed system from this paper is based on a local trust metric. The majority of other systems are based on a global metric (e.g. PageRank, eBay, Amazon, etc.). We mentioned in section 2 the proposals for local trust metrics. Some research works were realized concerning the personalization of PageRank (Haveliwala et al 2003) algorithm.

The closest metric to our research is *MoleTrust* proposed by (Massa, Avesani 2006). Analyzing this metric we have some observations that sustain our modeling point of view in StarTrust.

contradictory mode. This aspect is reflected in the trust value that A will associate to C. If C is evaluated in an unjust mode by B, in system will be other evaluations that may be favorable to C and will diminish the effect of B rating; also the reputation of C will not be strong affected. But to destroy a circuit from B to C may represents an eliminated information source for A, and we will obtain values that will not totally reflect the reality.

In MoleTrust, is introduced a factor named *trust_threshold*, that represents the threshold among the considered and un-considered ratings in trust computing. We mention that this factor will also affect trust propagation and the access to suitable resources.

Let us consider the following situation: a user A has no evaluation (explicit or implicit) associated to users B, C, D. A does not evaluated a resource R. In this case A may consider the reputation of system users.

We consider that B has evaluated with a big rating the resource R and B has a good reputation. Focusing on that, A will consider that R resource is good and will try to use it. But will discover that the resource is not that he need and then will evaluate B with 0.1. In MoleTrust such an evaluation (scaled in interval 0-1 become 0.02) will be effectively ignored and in this case the penalty of an evaluation is not possible to be realized. So, the preference of the user to do not take into account some resources evaluated by B is an aspect unsurprising in MoleTrust.

Other analyze was realized concerning the MoleTrust trust computing formula:

$$trust(u) = \frac{\sum_{i \in predecessors} (trust\_edge(i,u) * trust(i))}{\sum_{i \in predecessors} (trust(i))}$$

Use-case 1: we consider the following case:

Table 4. Explicit evaluations

Source User Id	1	2
Evaluated User Id	2	3
MoleTrust/StarTrust Rating	0.2/ 1	1/5

Using MoleTrust formula, trust that user 1 will provide to user 3 will be computed so:

$$trust(3) = \frac{trust(2) * trust\_edge(2,3)}{trust(2)} = 1,$$ in evaluation interval [0, 1].

To compute the factor we used was $P_{TC} = 0$. If we consider that to the users we can grant a certain trust level we may use for $P_{TC} = 1.5$. In this case: $WI\_UU(U_1,U_3)$=1,85.

Intuitive, the value obtained with StarTrust is more relevant than the value obtained with MoleTrust. If a user A will evaluate a user B with 1 (specifying the distrust in B) and B will evaluate C with 5, then is sure that A will not wish to evaluate C with 5 using only the experience of B.

Use-case 2: This example is assumed from (Massa, Avesani 2006) with MoleTrust metric and we specify some remarks using Star Trust metric.

Table 5. User-User explicit evaluations from (Massa, Avesani 2006)

Source User Id	1	2	2	4	4	5	5	4	6	7	8	8	9	10
Evaluated User Id	3	3	4	3	2	4	2	7	7	6	7	9	10	9
MoleTrust/ StarTrust Rating	0.9/ 4.5	0.6/ 3	0.5/ 2.5	1.0/ 5	0.9/ 4.5	0.1/ 0.5	0.8/ 4	0.9/ 4.5	0.9/ 4.5	0.5/ 2.5	1/ 5	0.8/ 4	0.7/ 3.5	0.3/ 1.5

As we observe in this case when only one arc will enter in the evaluated node, the trust value will be the trust value of the node that has a direct arc in 3, i.e. node 2. The trust of 1 in 2 is not used, being simplified.

In StarTrust in this case the value determined by 1 to 3 in [0, 5] interval will be:

$$WI\_UU(U_1,U_3) = \frac{1}{1 * MaxWorth}(WU(U_1,U_2),$$
$$*WE\_UU(U_2,U_3)) = 1$$

In (Massa, Avesani 2006) using MoleTrust from the point of view of user U_3 we have:

$$trust(3) = \frac{trust(2) * trust\_edge(2,3) + trust(1) * trust\_edge(1,3)}{trust(2) + trust(1)}$$
$$= \frac{0.8 * 0.6 + 1 * 0.9}{0.8 + 1} = 0.767$$

or 3.83 in scale [0, 5].We remark that metric does not compute values less than a certain threshold, so the evaluation from user 5 to 4 is ignored. If the value will be considered, then $trust(3) = 0.778$ or 3.89 in scale [0, 5].

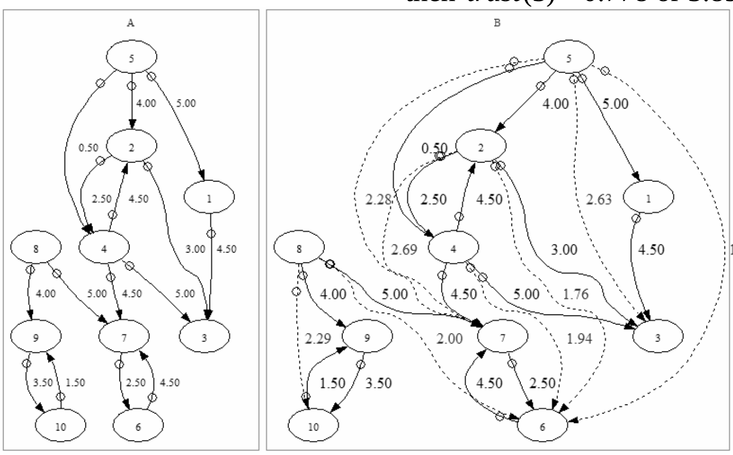

Figure 3. The graph represents the community composed by 10 users. A is the graph with explicit ratings with values for arcs in [0, 5] scale (see Table 5 for Mole Trust scale); B is the graph for explicit and implicit ratings obtained with StarTrust; continue arcs represents explicit evaluations and implicit evaluations are represented by dot arcs

Using StarTrust, we obtain trust propagation as in the Figure 3. The value $WI\_UU(U_5, U_3) = 2{,}64$ or 0.528 in interval [0, 1], for P_{TC} =1.5.

Using an empiric analyze, we remark that U_5 will express the distrust in U_4 giving a 0.5 rating. In the value of $WI\_UU(U_5, U_3)$ it can be find this evaluation which will determine a lower implicit rating of U_5 for U_3. For P_{TC} =4 we obtain $WI\_UU(U_5, U_3) = 3{,}95$. This big value of the parameter specifies that we have a community with a high trust level for members.

We also remark that depending on different online communities with different profiles StarTrust allows to realize an adaptation of trust computing depending on these situations.

5. Conclusions and future work

The paper presents a trust and reputation based model, able to help users from online communities to interact with appropriate users and resources. In these mode good decisions and few time-consuming actions concerning resource management can be realized.

We enumerate a set of consequences resulting from how the system was modeled.

- Resources relevant to a user (even those new) are visible in the top list of resources
- The system ensures that a user will see resources prioritized, in a similar manner with those which resemble
- Users who add *spam* resources will see more *spam* because the system groups users according to their preferences
- Users are encouraged to make proper evaluations

It will not happen as in eBay, where users give the most positive ratings of fear of possible revenge. In systems based on StarTrust metric, there are no good or bad ratings, there are interesting or uninteresting ratings from the point of view of users. The rating given by a user is pursue its goal, namely to quickly access important resources for it.

As we have seen with a trust metric, the trust can be propagated in the community. This is an advantage that can be used by a recommendation system. If we have a new user U evaluating many resources, through standard mechanisms those evaluations cannot be propagated. But if user U has evaluated a set of users, than using a trust metric as used in Star Trust, the system can associate a greater number of resources and the recommendation mechanism is more efficient.

Moreover, taking into account user-user evaluations, the system ensure a faster integration of new users in the system. Additionally, if they entered in the community by an invitation of an older member of the community, this invitation can be considered an explicit evaluation between users. Using StarTrust trust metric the system will be capable to recommend resources from the first moment.

The design of StarTrust will allow that our system can be integrated in different online communities as: education, e-health (Chiorean et all 2010), social networks, etc.

As future research direction we will study the behaviour of the model in real communities as medical and educational domains. Also, we shall study the reputation in an online community not limited to a given domain.

REFERENCES:

1. ALBOAIE, L. **PReS – Personalized Evaluation System in a WEB Community**, Proceedings of the International Conference on E-Business, 2008, pp. 64-69.
2. ALBOAIE, L., T. BARBU, **An Automatic User Recognition Approach within a Reputation System Using a Nonlinear Hausdorff Derived Metric**, Numerical Functional Analysis and Optimization, Pub. Taylor & Francis, Vol. 29, Issue 11 & 12, 2008, pp. 1240-1251
3. ALBOAIE, L., **Studies on Trust Modeling and Computation of Reputation in Online Communities**, Ph.D. thesis, Al. I. Cuza University, Iasi, 2009
4. ALBOAIE, L., S. BURAGA, **Trust and Reputation in e-Health Systems**, Proceedings of the International

Conference on Advancements of Medicine and Health Care through Technology; IFMBE Cluj-Napoca, vol. 26, 2009, pp. 43-46.

5. ALBOAIE, L., M.-F. VAIDA, **Modeling of Trust to Provide Users Assisted Secure Actions in Online Communities**, NDT, Communications in Computer and Information Science of Springer Lecture Notes, Prague, Series-87, 2010, pp. 369-382.

6. BERNERS-LEE, T., et al., **Uniform Resource Identifiers** (**URI**), General Syntax, RFC 2396, IETF, 1998.

7. BREABAN, M., L. ALBOAIE, H. LUCHIAN, **Guiding Users within Trust Networks Using Swarm Algorithms**, IEEE Congress on Evolutionary Computation (IEEE CEC 2009), 2009, pp. 1770-1777.

8. CHIOREAN, L. D., L. SUTA, M.-F. VAIDA, M. HEDESIU, **Medical Fusion Components for a Web Dedicated Application**, Studies in Informatics and Control, Vol. 19, Issue 4, 2010, pp. 435-444, ISSN 1220-1766.

9. GAMBETTA, D., **Trust: Making and Breaking Cooperative Relations**; **Can We Trust Trust**?, Basil Blackwell, 2000, pp. 213-237.

10. GOLBECK, J., **Personalizing Applications through Integration of Inferred Trust Values in Semantic Web-Based Social Networks**, Proceedings of the Semantic Network Analysis Workshop at the 4th Intl. Semantic Web Conference, Galway 2005.

11. GOLBECK, J., **Computing and Applying Trust in Web-based Social Networks** PhD thesis, Univ. of Maryland, 2005.

12. GOLBECK, J., **Computing with Social Trust**, Springer Publisher, 2009, pp. 338.

13. GUHA, R., **Open Rating Systems**, Technical report, Stanford Knowledge Systems Laboratory, Stanford, CA, USA, 2003.

14. HARDIN, R., **Trust and Trustworthiness**, Russell Sage Foundation, New York, 2002.

15. HARMON, A., **Amazon Glitch Unmasks War of Reviewers**, The New York Times, 14 February 2004.

16. JOSANG, A., R. ISMAIL, C. BOYD, **A Survey of Trust and Reputation Systems for Online Service Provision**, Decision Support Systems, Vol.43, no.2, Elsevier Science Publishers., 2007, pp. 618-644

17. LEVIEN, R., **Attack Resistant Trust Metrics**, PhD thesis, UC Berkeley, Berkeley, CA, USA, 2003.

18. MASSA, P., P. AVESANI, **Controversial Users Demand Local Trust Metrics: an Experimental Study on Epinions.com Community**, Proceeding of the 25th Conference, 2005, pp. 121-126.

19. MASSA, P., P. AVESANI, **Trust-Aware Bootstrapping of Recommender Systems**, ECAI'06 Workshop on Recommender Systems, 2006, pp. 29-33.

20. MASSA, P., P. AVESANI, **Trust Metrics on Controversial Users: Balancing Between Tyranny of The Majority and Echo Chambers**, Intl. Journal on Semantic Web and Information Systems, vol. 3(1), 2007, pp. 39-64.

21. MUI, L., M. MOHTASHEMI, A. HALBERSTADT, **A Computational Model of Trust and Reputation**, Proceedings of the 35th Annual Hawaii Intl. Conference on System Sciences, 2002, pp. 2431- 2439.

22. NURMI, P., **A Bayesian Framework for Online Reputation Systems**, AICT-ICIW’06, 2006, p. 121.

23. PAGE, L., S. BRIN, R. MOTWANI, T. WINOGRAD, The PageRank Citation Ranking: **Bringing Order to the Web**, Technical report, Stanford Digital Library Technologies Project, 1998.

24. RAHMAN, A., S. HAILES, **Supporting Trust in Virtual Communities**, System Sciences, Proceedings of the 33rd Annual Hawaii Intl. Conference on System Sciences, vol. 1, 2000, p. 9.

25. SABATER, J., C. SIERRA, **Social ReGreT, a Reputation Model Based on**

Social Relations, SIGecom Exchanges 3.1, 2002, pp. 44-56.

26. SEPANDAR, D. K., M. T. SCHLOSSER, H. GARCIA-MOLINA, **The Eigentrust Algorithm for Reputation Management in P2P Networks**, 12th Intl. Conf. on World Wide Web, 2003, pp. 640-651.
27. SUNSTEIN, C. R., **Republic.com 2.0**, Princeton University Press, 2009, p. 241.
28. DE TOCQUEVILLE, A., **Democracy in America**, The Library of America, New York, 1835-1840.
29. ZIEGLER, C., G. LAUSEN, **Analyzing Correlation between Trust and User Similarity in Online Communities**, 2nd Intl. Conf. on Trust Management, Springer, 2004, pp. 251-265.
30. WU, Z., X. YU, J. SUN, **An Improved Trust Metric for Trust-Aware Recommender Systems**, First Intl. Workshop on Education Technology and Computer Science, vol. 1, 2009, pp. 947-951.