

# Credibility Enhanced Reputation Mechanism for Distributed e-Communities

Eleni Koutrouli and Aphrodite Tsalgatidou

Dept. of Informatics and Telecommunications,  
National and Kapodistrian University of Athens  
e-mail: {ekou, atsalga} @ di.uoa.gr

**Abstract**— P2P communities are online communities of entities which offer services to each other without a central administration. Community members that need a specific service have to choose the transaction partner which they believe that will provide them with a required service of the expected quality; thus, they need mechanisms to support trust decisions regarding who they will transact with. P2P reputation systems provide trust mechanisms for P2P communities. Due to their decentralized and social nature, they are vulnerable to various types of attacks which distort their credibility and effectiveness. In our paper we first identify the credibility factors of a P2P reputation system. Then we describe a dynamic reputation mechanism for P2P communities, which integrates some of these credibility factors and which can be used as part of a comprehensive reputation system enhancing its robustness against some types of attacks. Simulation results show the effectiveness of our mechanism in relation to other reputation mechanisms which do not integrate such factors.

**Keywords-component;** P2P reputation systems, reputation attacks, reputation metric, e-community, credibility, P2P systems

## I. INTRODUCTION

Peer-to-Peer (P2P) systems and applications are attracting a lot of attention nowadays, as they mimic human communities and support useful community tasks (e.g. file sharing, collaboration, and e-commerce). Due to their social and decentralized nature, trust plays an essential role for their functionality. P2P reputation systems have emerged in order to satisfy this need for trust inference by providing trust mechanisms for P2P applications. However, reputation systems themselves are targets of multiple kinds of attacks which should be taken into consideration during the design of the former in order to be effective.

In this paper, we propose a reputation mechanism for P2P e-communities of experts who want to collaborate and use a variety of services offered by the members of the community to each other. This mechanism is intended to be used in the implementation of a reputation system which is immune to potential threatening attacks, such as bad mouthing and strategic changes of transactional behaviour. In order to achieve this goal we have taken into account credibility considerations, which have been pointed in previous research as [1] and [2]. The proposed reputation mechanism incorporates a dynamic reputation inference algorithm (reputation metric) that integrates direct and indirect transactional information, takes into consideration

the recommendation reputation of recommenders, and gives greater weights to the more recent and more credible recommendations.

The rest of the paper is organized as follows: the next section presents the main concepts of a reputation system for P2P communities; it also presents the factors that determine the credibility of such a reputation system and describes some types of potential attacks that can undermine its credibility and effectiveness. The proposed reputation mechanism is described in section 3. The results of some early simulation experiments as preliminary proof of concept are presented in section 4. In section 5 we refer to related work. Finally, we discuss open issues and outline our future work.

## II. P2P REPUTATION SYSTEMS

### A. Main Concepts of a P2P Reputation System

A decentralized reputation system comprises entities that play interchangeably the roles of *trustor*, *trustee* and *recommender*. The *trustor* is an entity which wants to make a *trust decision* regarding whether to participate or not in a *transaction* with another entity, the *trustee*. A transaction can involve accessing or allowing access to a resource, e.g. a file, buying or selling goods, collaboration between two entities for a project, etc. The *recommender* is the entity that provides the trustor with information regarding the trustworthiness of the trustee; this information is known as *recommendation*.

To make a trust decision the trustor tries to predict the future behaviour of the trustee by forming a view of the trustee based on experience about its earlier actions. This subjective view comprises the trustee's *reputation* or *trustworthiness* from the trustor's point of view. To form a reputation view, the trustor needs to gather experience information, by referring to its own earlier experience with the trustee and / or by acquiring it from other entities in the form of *recommendations*. Recommendations can be based on the *recommender's* personal experience alone, or on a combination of personal experience and recommendations from others. A recommendation is either a *rating* describing a single transaction experience, or an *opinion* formed by the outcome of several direct transactions between the recommender and the trustee and possible outside experience. The aggregation of personal experience and recommendations regarding the trustee results in calculating

the trustee's reputation value, which can be translated in a way that facilitates a *trust decision*, by comparing either the trustee's reputation value with a specific threshold (e.g. [3], [4], [5], [6]) or the trustworthiness of different peers in order to select the most reputable entity (e.g. [7]).

The *reputation* of a peer is *context-specific*, as it depends on the kind of provided service. Reputation also depends on *time*, as the behaviour of peers is dynamic and recent transactions are often considered more important for reputation calculation than older ones.

A rational use of recommendations is to select and weigh them based on the *credibility of the recommenders*. A way to achieve that, includes comparing the recommendation with the actual satisfaction obtained by the transaction with the trustee and evaluating the credibility of the recommender accordingly. The available information (both direct transactional information and recommendations from others) should be transformed to a useful reputation value using a calculation method which can be either deterministic, probabilistic or based on fuzzy logic [8]. Calculated reputation values are stored either locally by the trustor or the trustee or by special peers and are sent to other interested parties either upon request, or by dissemination.

### B. Potential Attacks against P2P Reputation Systems

An effective reputation system is expected to estimate the peers' trustworthiness as accurately as possible in order to lead to the right trust decisions. Thus, credibility is an essential property of a reputation system, and refers to the confidence that can be placed on its effectiveness. Entities participating in reputation systems can distort the credibility of the latter in various ways, either deliberately or not, isolated or in cooperation with others. Reputation attacks or misbehaviour belong to the following three main categories:

*Unfair recommendations:* Entities can spread unfair ratings for other entities or can do it with cooperation with each other to maximize the effect of the attack. Unfair ratings can be due to lying, misjudging the outcome of a transaction, or making a mistake. The case of lying when providing recommendations is referred to as *bad mouthing*. A malicious peer can 'bad-mouth' other peers (i.e. spread fraudulently low recommendations for them) in order to unfairly reduce their reputation, so as to increase its own reputation when related to them [11]. *Inaccurate recommendations* belong also to the category of unfair recommendations: These can be due to having incomplete information, e.g. a peer which sends an opinion-based recommendation about another peer may have little experience with it, and, thus a *weak confidence* about the opinion. Such a recommendation cannot be considered as accurate as it involves a high level of *uncertainty*.

*Strategic behaviour (Traitors):* Peers may strategically have an inconsistent behaviour that can lead to an incorrect calculation of their reputation allowing them to misbehave and still keep a high reputation. They can, for example misbehave part of the time or towards a subset of peers (*oscillating behaviour*) or change their behaviour suddenly

or periodically (*sudden changes in behaviour*), as described in [12], [13].

*Identity management related attacks:* When the identity scheme permits the use of multiple identities by the same peer, a malicious peer can have a dishonest behaviour and then *escape* its low reputation by entering the system with a new identity. A peer may also create multiple identities and use them to spread negative recommendations about a single user [14]. Weak authentication mechanisms and / or lack of data integrity protection may also favour *man-in-the-middle attacks*, where intermediate peers tamper with reputation information passing through them.

The reputation mechanism that we propose aims to defend the first two categories of attacks. In order to achieve this goal, we considered a number of credibility factors which we present in the following.

### C. Credibility Factors of P2P Reputation Systems

Before describing the proposed reputation mechanism we would like to outline a set of factors that affect the credibility of a reputation. These factors have been taken into account in the proposed solution and are as follows:

*Recommendation Creation and Recommendation Content:* Recommendation information should accurately reflect the quality of the transactions with the trustee. In the case of opinion-based recommendations the *number* and the *volatility* of aggregated ratings influences the credibility of the recommendation. The more the ratings which are aggregated to produce an opinion, the more credible the recommendation is. Furthermore, a high volatility of the level of satisfaction obtained from the evaluated transactions is an indicator that the recommendation has low credibility. Therefore, the *confidence* a recommender has for its opinion-based recommendation, depending on the *amount* and the *volatility* of information it has, is an important information element that should be provided with the recommendation. *Time* is also an important element for both rating-based recommendation (as a means to prove the existence of a transaction associated with a rating) and opinion-based recommendations (in order to evaluate individual ratings based on their *recency*).

*Recommendation Selection:* The quality of recommendations depends highly on the quality of the recommenders who need to be the most relative and credible; therefore, attention needs to be paid to keeping track of the *credibility* of the *recommenders* and using it to weight recommendations.

*Reputation Reasoning:* The algorithm used for the aggregation of direct experience and recommendations in order to calculate a reputation value should take into account the *recency* and *context* of recommendations and the *confidence* that can be placed both on a recommendation and on a peer's direct experience evaluation.

## III. REPUTATION MECHANISM FOR E-COMMUNITIES

In this section we describe an e-community of experts, a reputation mechanism that can support such an e-community as well as the formulae used to calculate peers'

reputation. Our reputation mechanism deals with most issues discussed in Section II, namely recommendation formation, recommendation request procedure, direct and indirect reputation information, etc.). It is thus part of a comprehensive reputation system which will deal with the rest of the discussed issues, such as recommendation credibility estimation, trust decision method, etc. and also with implementation issues, such as identity scheme implementation, cryptographic methods, overlay implementation, etc.

#### A. e-Community Description

An e-community of experts is a community of individuals which offer services to each other, such as exchanging ideas / papers / pieces of code, engaging in future synergies for a project, etc. Each expert has an expertise in one or more fields, e.g. Programming, Communications, Economics, etc. and may offer a number of services in some of these fields (e.g. paper review, paper recommendation, advise, code provision). The level of expertise is expressed in a particular scale, e.g. a range of integers in  $\{1, \dots, 5\}$ , where numbers express levels of expertise in ascending order. A member of the community can claim the level of expertise she has in each field, by, for example, sending advertisements about herself in a Distributed Hash Table (DHT) (e.g. Chord overlay [15]).

Peers can query the community to find experts in a particular field by searching the available advertisements which are distributed in the overlay. In order to ask a service from a particular expert and make, thus, a transaction with her, a community member should estimate a reputation measure which will indicate the expert's capability to provide the required service of an acceptable quality.

Every peer keeps information regarding its transactions and the QoS it receives in each transaction, in a table called Local Transaction Evaluation table (LTE table).

TABLE I.. LOCAL TRANSACTION EVALUATION TABLE (LTE TABLE)

Peer Id	Time	Field of expertise ( $f_i$ )	Service Id	ServiceOutcome

where:

*Peer Id*: Id of the counterparty in a transaction

*Time*: time of the transaction

*Field of expertise ( $f_i$ )*: the field where a peer has an expertise

*Service Id*: Id indicating the type of service

*ServiceOutcome*: a rating regarding the evaluation of a transaction. Such a rating is a real number in  $[0,1]$ . The higher (lower) the level of satisfaction obtained by a transaction the closer to 1 (0) the rating is.

Every peer assigns each type of the services offered by the community a particular level of importance, which is symbolized as *ServiceImp* and is kept locally in a table called Service Importance table (SI table).

TABLE2. SERVICE IMPORTANCE TABLE (SI TABLE)

Service Id	ServiceImp

The evaluation of a transaction (*TransEval*) is a function of *ServiceImp* and *ServiceOutcome*:

$$TransEval = f(ServiceOutcome, ServiceImp).$$

In the proposed reputation mechanism *ServiceImp* takes values in the range  $[0,1]$  and is used to weigh *ServiceOutcome* when evaluating the transaction:

$$TransEval = ServiceImp * ServiceOutcome \quad (1)$$

Each peer also keeps a Recommendation Reputation Value table (RRV table) which holds reputation values regarding the recommending behaviour of peers from which it has received recommendations. We refer to these kind of reputation values as **recommendation reputation** values.

TABLE III.. RECOMMENDATION REPUTATION VALUE TABLE (RRV TABLE)

Remote PeerId	RecRep Value

After transacting with a peer (trustee), the trustor (peer **A**) estimates the recommendation reputation values of its recommenders based on the similarity between the recommendations it has received by them for the trustee and its own evaluation of the transaction. A peer **B** with a high *RecRep* value in the RRV table of peer **A** is considered by **A** as a credible recommender.

When a peer **A** wants to estimate **B**'s reputation regarding the services it provides in field  $f_x$  in order to decide whether to make a transaction with it, the reputation calculation mechanism is determined according to the amount of available transactional information. So, the overall reputation of a peer comprises direct and indirect reputation, as described in the following cases.

**1st Case: Adequate local transactional information:** Peer **A** looks into its LTE table in order to check if it has adequate transactional information regarding **B** in the field of expertise  $f_x$  in order to reach a trust decision. To do that, **A** estimates

- the *direct reputation* of **B** in  $f_x$  and
- a *confidence measure* for this direct reputation value based on the *amount* and *volatility* of the available information.

(the calculation of the direct reputation and confidence are described in the following section)

If **A** has adequate information regarding **B**, it sends its transaction query to it only if its direct reputation is higher than a threshold.. After the transaction is completed, peer **A**

enters a related evaluation value for the transaction (Service Outcome) in its own LTE table.

**2nd Case: Not enough local transactional information:** If peer **A** has some transactional information for peer **B** in the field of expertise  $f_x$  with low confidence (minimum than a threshold) or if it does not have information at all, then it sends recommendation queries for **B** to the neighbouring peers which have a recommendation reputation value higher than a minimum threshold.

Peers which have the required information regarding **B**'s transactional reputation, send them to the requestor aggregated as an opinion, consisting of a pair  $\langle \text{recommendation}, \text{confidence} \rangle$ . The requestor (peer **A**) aggregates the received recommendations and estimates the indirect reputation of the peer **B**. Then it estimates the overall reputation value of **B** by aggregating the direct and indirect reputation values and sends a transaction query to it only if its overall reputation is higher than a threshold. After the transaction is completed, peer **A** updates the recommendation reputation values (in its RRV table) of the peers from which it received recommendations regarding peer **B**, according to the QoS evaluation of the transaction with **B**.

### B. Reputation Calculation

*Calculation of Direct Reputation:* A peer **A** estimates the direct reputation value of a peer **B** based on the weighted average of the transaction evaluation values which the peer has estimated regarding its transactions with **B**, where each transaction evaluation value has been weighted by a time decay factor. The formula for direct reputation calculation is shown in (2).

$$DirectRep_{A,B} = \frac{1}{\sum_{i=1}^n f(t_i, t)} \sum_{i=1}^n f(t_i, t) TransEval_{t_i, B} \quad (2)$$

where

$n$  is the total number of transactions between **A** and **B**,

$TransEval_{t_i, B}$  is the transaction evaluation value that **A** has estimated regarding its transaction with **B** at time  $t_i$  according to formula (1)

$f(t_i, t)$  is the **decay function** that weights evaluation values of transactions that took place at time  $t_i$ , giving higher weight to values closer to current time  $t$ . Specifically

$$f(t_i, t) = e^{-Dt} \quad (3)$$

where

$t_i$  is the time when the  $i_{th}$  transaction between the trustor and the trustee took place

$t$  is the current time

$Dt$  is the time interval between time  $t_i$  and the current time  $t$ .

For each direct reputation value a **confidence value**  $Conf_{A,B}$  is calculated which expresses the confidence that the

trustor **A** can place to the reputation value it has calculated for **B**, based on its own transactional information. Based on this value, the trustor can decide whether the available direct information is credible enough or recommendations regarding the trustee need to be requested too.

*Confidence calculation* takes into considerations the following three factors:

(i) *Number of transactions:* If this number is high the confidence is high too. We define the Number of Transactions factor NT as follows:

$$NT = \begin{cases} 1, & \text{if } n \geq N \\ \frac{n}{N}, & \text{otherwise} \end{cases} \quad (4)$$

where

$n$  is the number of transactions between **A** and **B**, and  $N$  is a threshold for the number of transactions; the choice of  $N$  depends on the requirements of the application.

(ii) *Volatility of the transaction evaluation values.* Volatility is calculated using the following formula:

$$Dev_{A,B} = \sum_{i=1}^n \frac{|TransEval_{t_i, B} - DirectRep_{A,B}|}{n} \quad (5)$$

where

$n$  is the number of transactions between **A** and **B**,

$TransEval_{t_i, B}$  is the transaction evaluation value that **A** has estimated regarding its transaction with **B** at time  $t_i$  according to (1)

$DirectRep_{A,B}$  is the direct reputation value that the trustor **A** has estimated for **B** using (2)

The value of  $Dev_{A,B}$  is in the range [0, 1]. A deviation value near 1 indicates a high variability in the rating values (that is, a low confidence on the calculated direct reputation value), whereas a deviation value close to 0 indicates a low variability (that is, a high confidence).

(iii) *Age of transactions with the trustee.* It refers to the time of the last transaction that has been evaluated and taken into consideration in the reputation value. This is done by integrating the decay function in confidence calculation, as shown in the following formula:

$$Conf_{A,B} = NT * (1 - Dev_{A,B}) * e^{-Dt} \quad (6)$$

where

$Dt$  is the time interval between the current time and the time of the last transaction included in the evaluated transactions,

$NT$  is the Number of Transactions factor estimated by formula (4).

*Calculation of Indirect Reputation:* The indirect reputation value that the trustor **A** calculates for the trustee **B** is the aggregated recommendation information that **A** collects from recommenders. A recommendation consists of a reputation value estimated by the recommender regarding the trustee and the associated confidence value. In the proposed reputation system, the reputation value provided as a recommendation is the direct reputation valued regarding the trustee based on the transactional information contained in the recommender's LTE table. The confidence value indicates how much confidence the recommender can put on the recommendation that it provides and is calculated by (6). The recommendation that a recommender  $\rho$  gives **A** regarding **B** is thus represented by the tuple  $\langle RecommendationValue_{\rho,B}, Conf_{\rho,B} \rangle$ .

After collecting recommendation information regarding **B** from the queried recommenders, **A** calculates the Indirect Reputation of **B** using the following formula:

$$IndirectRep_{A,B} = \sum_{\rho=1}^k \frac{RecRep_{\rho} * (RecommendationValue_{\rho,B} * Conf_{\rho,B})}{k} \quad (7)$$

where

$k$  is the number of recommenders,

$RecRep_{\rho}$  is the recommendation reputation of the recommender  $\rho$ , stored in the RRV table of peer **A**

$RecommendationValue_{\rho,B}$  is the recommendation given by the recommender  $\rho$  for trustee **B**, calculated based on the recommender's direct experience with the trustee using formula (2)

$Conf_{\rho,B}$  is the confidence put by the recommender  $\rho$  to the recommendation value that it provides regarding **B**. It is calculated using formula (6).

*Calculation of Overall Reputation:* After having computed the direct and indirect reputation values regarding **B**, the trustor **A** can calculate the overall reputation of **B** by aggregating these reputation values while assigning different weights to them. The weight  $\alpha$  assigned to direct reputation value is a value in the range [0,1] and indicates how much the trustor wishes to take into account its own transactional information. Indirect reputation is weighted by  $(1-\alpha)$ . Overall reputation of **B** is thus given by the following formula:

$$OverallRep_{A,B} = \alpha * Conf_{A,B} * DirectRep_{A,B} + (1-\alpha) * IndirectRep_{A,B} \quad (8)$$

where  $\alpha$  is a weight given to direct reputation and  $(1-\alpha)$  is the weight given to indirect reputation.

After each transaction, the recommendation reputation values of all recommenders that have given the trustor recommendations for the trustee are updated. This is done by comparing the transaction evaluation value with the recommendations given by the various recommenders. If  $|TransEval_{A,B} - Recommendation_{\rho,B}|$  is higher than a threshold  $\theta$  which is defined by the trustor, then  $RecRep_{\rho}$

will be decreased. The formulae for calculating Recommendation Reputation values are out of the scope of this paper.

### C. Preliminary proof of concept

We have conducted three groups of simulation experiments, in order to show the impact on the effectiveness of our reputation metric of three factors: *time decay function*, *confidence* and *recommendation reputation*. More specifically, we created some scenarios of peers' behaviour, as described in the following, and simulated them by creating views of the relative reputation information.

In the first group of our simulation experiments, we examined how our reputation metric resists *traitors attacks*, where a malicious peer provides services of a high quality for a period of time in order to acquire a high reputation and then changes its behaviour and provides services of lower quality. In order to do so, we simulated such a behaviour in two peers' history of transaction with a specific trustor. In the proposed reputation system peers which suddenly decrease the quality of their transactional behaviour cannot gain from the high evaluation values that have been given by their counterparties in the past, as their reputation is defined mostly based on their recent bad behaviour. This is shown in Figure 1, where the evaluation values of the transactions conducted by the trustor with two different peers, are modified according to their weighting with the time decay function. The weighted evaluation values, which are then used for the reputation calculation of the trustees, decrease as we go back to the time.

In the second group of simulation experiments, we examined how the confidence factor can help against the *oscillatory behaviour*. For this purpose, we simulated the recommendations of nine peers regarding a specific trustee which had exhibited an oscillatory transactional behaviour in the past. As a result of this behaviour, some peers have provided recommendations with low confidence due to the high variability of ratings given to the trustee. The recommendation values provided by these peers are weighted with the associated confidence values. For better understanding the impact of confidence weighting, we assumed that all recommenders have an invariant recommendation reputation. Figure 2 shows how the recommendations provided by recommenders are weighted according to the confidence values associated with recommendations. In cases of recommendations with low confidence, the relative weighted recommendations are low too, and so is their impact on the indirect reputation calculation of the trustee.

In the last group of simulation experiments, we examined how recommendation reputation can help against *bad mouthing*. In this group of experiments we simulated a set of nine recommenders with a varying recommendation reputation from the trustor's point of view. We assumed that the trustor acquires recommendations from them and that all recommenders have the same level of confidence for their recommendations. This assumption was made to better exhibit the impact of the weights of recommendations on the recommendation reputation of recommenders when

calculating the indirect reputation of the trustee. A fraction 30% of the recommenders had bad recommendation reputation in the RRV table of the trustor, as they had provided inaccurate recommendation information in the past. All recommendations were weighted with the recommendation reputation of the recommenders, so recommendations coming from low reputable recommenders are weighted the least. This is exhibited in Figures 3a and 3b, which show how the recommendations acquired by the trustor from a group of recommenders for trustees p1 and p2 are modified according to the recommendation

trustworthiness of the recommenders. In both examples the modified recommendation values are then used for the indirect reputation computed by the trustor, giving more importance to recommendations from high reputable recommenders.

We aim at continuing our experiments with more sophisticated threat scenarios in order to better choose the right time decay function and the weights of direct and indirect reputation in the overall reputation calculation.

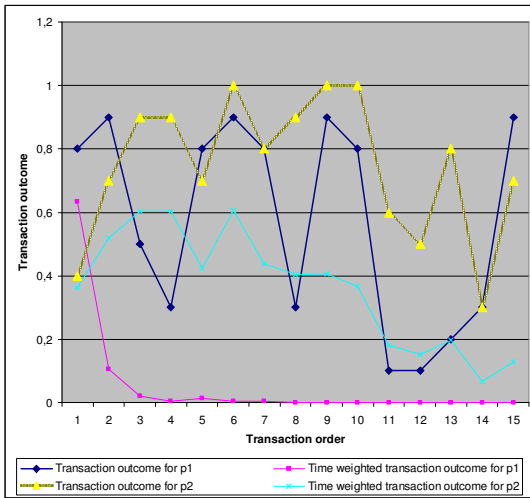


Figure 1. Time Weighting of Transaction Outcome Values for p1 and p2

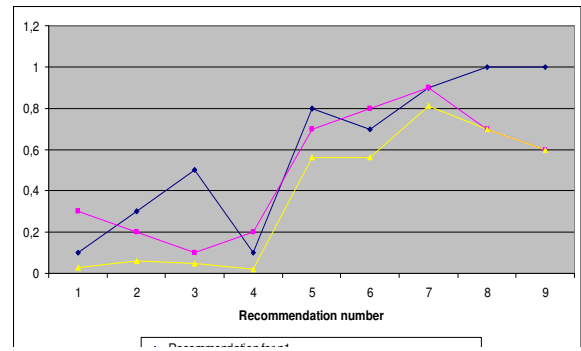


Figure 2. Weighting Recom. Values with Confidence of Recommender

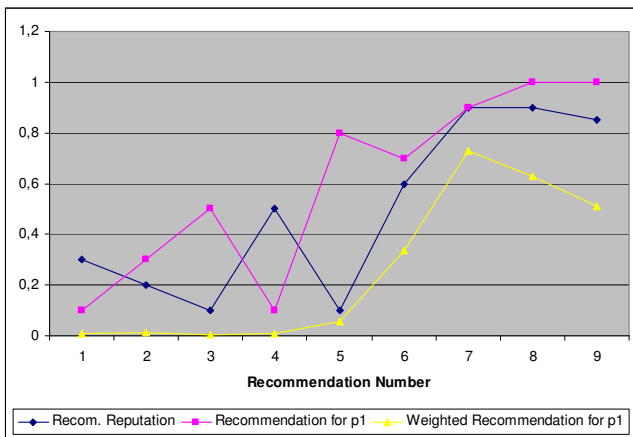


Figure 3. Weighting Recommendation Values for p1 with Confidence of Recommender

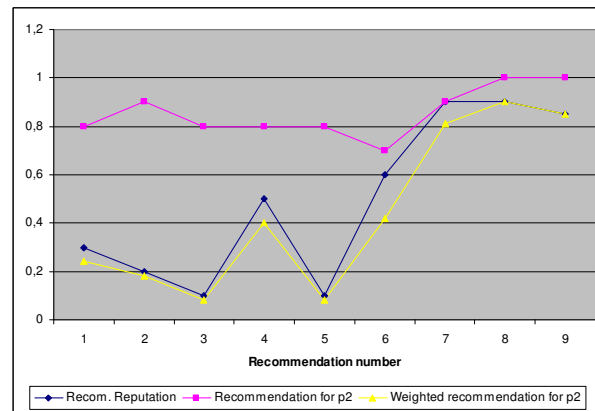


Figure 4. Weighting Recommendation Values for p2 with Recommendation Reputation

#### IV. RELATED WORK

A quite large amount of research work is found in the literature regarding the following two axes which we consider relative to our own work: a) reputation systems for e-communities, b) dynamic reputation metrics.

As the first axis is concerned, various reputation systems have been proposed for P2P communities (such as [3], [5], [6], [9] and [10]), dealing with various components of reputation systems for e-communities. For example, Xiong and Liu [3] present a distributed reputation system and describe the way reputation is calculated, stored and distributed. Dillon et al. [6] present a dynamic reputation metric which incorporates recommendation reputation, while Song et al. [10] focus on a reputation calculation method based on fuzzy logic and propose the use of an overlay for reputation information storage and retrieval. Lee et al. [9] propose a transitive recommendation mechanism where the trustee itself should provide the trustor with its own reputation value which calculated based on a chain of recommendations between the trustor and itself. Sabater and Sierra [5] propose a more comprehensive reputation system for e-communities which deals with an elaborative reputation calculation method, which takes into consideration various sources of information and incorporates social relationships in the recommendation selection method. The aforementioned works focus on a variety of issues such as reputation information storage [3], reputation information transitivity [9], incorporation of social relationships in reputation estimation [5]. Our work, when compared with those, has a different focus. Specifically, having examined the most important attacks against reputation systems, we focused on defining an optimal reputation inference algorithm (reputation metric), which can be used for the effective functionality of an e-community and which can mitigate these attacks. Other components of our reputation system, such as recommenders selection, recommendation reputation estimation, etc. which are not presented in this paper will be developed with similar security considerations in mind..

Furthermore, a number of approaches for defining a dynamic reputation metric to penalize sudden changes in behaviour and oscillatory behaviour is found in the literature. Duma et al. [12] propose a reputation metric where: a) negative ratings are weighted more than positive ratings and b) a penalty factor is used, which incorporates the difference between the calculated reputation of a peer before transacting with it and its reputation after the evaluation of the transaction. By using such a dynamic reputation metric, the cheating behaviour will quickly be reflected in the reputation of the misbehaving peers; at the same time these peers will need more work to recover their initial reputation after performing malicious actions. So sudden changes in behaviour and oscillatory behaviour are discouraged as they will be quickly detected and penalized. Gan et al. [16] propose a similar penalty factor which measures the level of oscillatory behaviour of a peer and is incorporated in the

reputation metric, so as to reputation of a peer will be continuously decreasing if the peer oscillates. In [13] the performance of peers is monitored in consequent time periods. In case of sudden changes of a peer's behaviour, the peer's reputation is decreased in such a way that low reputable peers will be able to increase their reputation gradually, whereas high reputable peers will find it more difficult to do so due to their severe punishment. In our reputation system we deal with oscillatory behaviour and sudden changes in behaviour by using the time decay function and the confidence assigned to direct reputation and recommendation values.

Furthermore, similarly to our proposed reputation metric, a number of reputation systems proposed in the literature weigh recommendations based on the honesty of recommenders when providing recommendations (e.g. [6], [17], [18] and [19]). In [6] each peer calculates the recommender's trustworthiness regarding the recommendations it gives, as the difference between the given recommendation and the trustor's evaluation of its transaction with the trustee. In [17] records are kept for the recommendation trustworthiness of a peer; these records are updated only in case the reputation of the trustee is updated after a transaction. In [18] and [19] credibility ratings are calculated by the trustor based on the received recommendation and the result of the transaction with the recommended entity. These credibility ratings are used for recommenders selection in [18] and for weighting recommendation in the reputation calculation process in [19].

#### V. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a reputation mechanism for an e-community, using a scenario of an experts e-community. The focus of our work was the definition of a credibility-enhanced dynamic reputation calculation metric, which can help against some major reputation attacks. The proposed reputation metric incorporates various sources of information and aggregates them by assigning weights that express their importance. More specifically, transaction ratings are weighted according to the time the transaction took place and recommendations are weighted according to a) the trustworthiness of the recommender regarding its recommendation behaviour and b) the confidence of the recommender regarding its recommendation. Confidence measures are associated to recommendations and direct reputation values. By incorporating confidence and the time decay function in our reputation metric, we aim at dealing with *strategic changes of transactional behaviour* which intend to harm other peers while the attacker maintains its good transactional reputation. Keeping and updating recommendation reputation values for peers and incorporating them in the overall reputation calculation helps against *bad mouthing* attacks. The proposed reputation metric is *dynamic* because of the time considerations on one hand and the possibility to use different weights for direct

and indirect reputation when calculating the overall reputation of a peer.

Last, we proposed the design of an experts e-community where:

1. Each peer sends advertisements for its expertise and the services it can provide in an overlay.
2. Experts are searched based on a particular expertise and are chosen as service providers based on their reputation.
3. Context is incorporated in reputation calculation, by proposing the calculation of reputation per field of expertise.

As a future work we aim at designing a secure incentive-based recommendation exchange mechanism that will be incorporated in a comprehensive reputation system for e-communities. The main considerations will be the provision of incentives for honest recommendations as well as the resistance to other threats that can target reputation systems.

#### REFERENCES

- [1] Ruohomaa, S., Kutvonen, L., and Koutrouli, E., "Reputation Management Survey", 2<sup>nd</sup> International Conference on Availability, Reliability and Security, 2007, pp. 103--111
- [2] Hoffman, K., Zage, D., and Nita-Rotaru, C., "A survey of attack and defense techniques for reputation systems", ACM Computing Surveys, 42, 1 (Dec. 2009), pp. 1--31. DOI= <http://doi.acm.org/10.1145/1592451.1592452>
- [3] Xiong, L., and Liu, L., "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities", IEEE Transactions on Knowledge and Data Engineering 16, 7 (July 2004), pp. 843--857
- [4] Despotovic, Z., and Aberer, K., "Maximum Likelihood Estimation of Peers' Performance in P2P Networks", 2nd Workshop on the Economics of Peer-to-Peer Systems, Cambridge, MA, USA, 2004
- [5] Sabater, J. and Sierra, C., "Social ReGreT, a reputation model based on social relations", ACM SIGecom Exchanges, 3, 1 (Dec. 2001), pp. 44--56. DOI= <http://doi.acm.org/10.1145/844331.844337>
- [6] Dillon, T.S., Chang, E., and Hussain, F. K., "Managing the Dynamic Nature of Trust", IEEE Journal Of Intelligent Systems 19, 5 (Sept/Oct 2004), pp. 79--82
- [7] Aberer, K., and Despotovic, Z., "Managing trust in a peer-2-peer information system" 10th International Conference on Information and Knowledge Management (CIKM), Atlanta, 2001
- [8] Chang, E., Dillon, T., Hussain, F. K., "Trust and Reputation for Service-Oriented Environments", Technologies for Building Business Intelligence and Consumer Confidence. John Wiley & Sons, Chapter 10.
- [9] Lee, S., Sherwood, R., and Bhattacharjee, B., "Cooperative peer groups in Nice", 22nd Annual Joint Conference on the IEEE Computer and Communications Societies, 2003
- [10] Song, S., Hwang, K., Zhou, R., and Kwok, Y.-K., "Trusted P2P Transactions with Fuzzy Reputation Aggregation", IEEE Internet Computing Magazine, Special Issue on Security for P2P and Ad Hoc Networks, Nov/Dec 2005, pp. 24--34
- [11] Dellarocas, C., "Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behaviour", 2nd ACM Conference on Electronic Commerce, 2000
- [12] Duma, C., Shahmehri, N., Caronni, and G., "Dynamic Trust Metrics for Peer-to-Peer Systems", 2nd International Workshop on P2P Data Management, Security and Trust, 2005, pp. 776--781
- [13] Dariotaki, Th., and Delis, A., "Detecting Reputation Variations in P2P Networks", 6th Workshop on Distributed Data and Structures, 2004
- [14] Douceur, J. R., "The sybil attack", 1st International Workshop on Peer-to-Peer Systems, 2002
- [15] Stoica, I., Morris, R., Liben-Nowell, D., Karger, D. R., Kaashoek, M. F., Dabek, F., and Balakrishnan, H., "Chord: a scalable peer-to-peer lookup protocol for internet applications", IEEE/ACM Transactions on Networking 11, 1 (Feb. 2003), pp. 17--32.
- [16] Gan, Z., Li, Y., Xiao, G., and Wei, D., "A Novel Reputation Computing Model for Mobile Agent-Based E-Commerce Systems", 2<sup>nd</sup> International Conference on Information Security and Assurance (ISA 2008), 2008, pp. 253--260
- [17] Selcuk, A. A., Uzun, E. and Pariente, M. R., "A Reputation-Based Trust Management System for P2P Networks", 4th International Workshop on Global and Peer-to-Peer Computing, 2004
- [18] Zhao, H., and Li, X., "H-Trust: A Robust and Lightweight Group Reputation System for Peer-to-Peer Desktop Grid", 28th International Conference on Distributed Computing Systems Workshops, 2008, pp. 235--240
- [19] Huynh, T. D., Jennings, N. R. and Shadbolt, N. R., "On Handling Inaccurate Witness Reports", 8th International Workshop on Trust in Agent Societies, Utrecht, Netherlands, 2005