# A Reputation-based Trust Model with Fuzzy Approach and $D_{p,q}$-Distance Technique for Peer-to-Peer Networks

Bagher Rahimpour Cami
Faculty of Computer & IT Engineering
Mazandaran University of Science & Technology,
Babol, Iran

Hamid Hassanpour
Faculty of Computer & IT Engineering
Shahrood University of Technology
Shahrood, Iran

## ABSTRACT
Peer-to-peer networks have become increasingly popular in the recent years. In an open peer-to-peer network peers often have to interact with unknown peers and need to manage the risk in their communications. It is very important for peers to select a trustworthy peer to accomplish a task. Peers must be able to determine the trustworthiness of other peers to increasing uncertainty and risk. Thus trust policies and trust evaluation mechanisms are needed for quantifying and comparing the trust worthiness of peers. In this paper we propose a trust evaluating model based on reputation and statistical technique. In the proposed trust model the measure of trust is evaluated with $D_{p,q}$-distance technique. This technique uses quad set of positive experience and negative experience and recommendation of other peers for evaluating and comparing of trustee peers.

## General Terms
Security and Trust.

## Keywords
P2P Network; Trust; Reputation; Fuzzy Trust.

## 1. INTRODUCTION
Peer-to-peer networks can be seen as truly distributed computing application in which peers communicate directly with one another to exchange information, distribute task, execute transaction, knowledge sharing, file sharing, game playing, or ecommerce. Some popular systems that are currently in operation include SETIQ home [1, 2], Gnutella [1, 3] and Freenet [1, 4]. Their open, distributed and anonymous nature makes them very vulnerable against malicious users who provide bad responses to requests from other peers [5]. In an open P2P networks, peers often have to interact with unknown or unfamiliar peers and need to manage the risk that is involved with the interactions without the presence of trusted third parties or trust authorities [1].

However, the open and anonymous nature of these networks lead to a complete lack of accountability for the content a peer puts on the networks, opening the door to abuse of these networks by malicious peers [6]. Attacks by anonymous malicious peers have been observed on today's popular peer-to-peer networks. For example, malicious users have used these networks to introduce viruses such as the VBS, Gnutella worm [7]. How to distinguish the validity of a resource and how to verify the authenticity of the content of a resource are both problems that might be faced. In order to solve these problems trust model have emerged as an important risk management mechanism in online communication [8]. The main goal of trust model is to detect malicious or unreliable entities in the network [9].

Most of approaches to trust models focus on reputation. Reputation-Based trust model uses experience or the experiences of others as recommendation, possibly combined to make trust decision about an entity [10, 11, 12 and 13]. Most research on reputation-based trust utilizes information such as community-based feedbacks about past experiences of peers to help making recommendation and judgment on quality and reliability of the transactions [14].

Each Reputation-Based trust Models has specific approach and mechanism to evaluate the trust. For example, eBay's feedback scheme [15, 16], Peer Trust rating framework [15, 17], Eigen Trust (page ranking) global trust ranking systems [15, 18], PET personalized economic model [15, 19] and fuzzy trust [15, 20] are some of Reputation-Based trust model.

In our approach, each peer has some metrics to judge about a provider peer. The positive experience and the negative experience and the positive recommendation and the negative recommendation are metrics for a peer to judge about another peer of networks.

In this paper we propose a trust model for aggregation of reputation metrics and provide a trust score for comparing peers. It uses the $D_{p,q}$-distance algorithm for aggregation metrics. These metrics provide a fuzzy set for a peer to evaluate the trustworthiness of other peers. The rest of this paper is structured as follows. In Section 2 we present the $D_{p,q}$-distance algorithm. Section 3 presents the trust model. Section 4 shows the result of experiments. Section 5 concludes the paper.

## 2. FUZZY APPROACH TO TRUST MODEL
Trust has been defined in various ways [21]. The following is the Gambetta's [22] which is a well-known definition of trust: trust is a particular level of the subjective probability with which an entity will perform a particular action, both before we can monitor such action and in a context in which it affect own action. A number of trust model have been proposed. Some models depend only to user's rating to compute the trust value [6, 16], and others get the trust values by observing the behaviors of the entity over some period [10, 11, 13]. In this paper we proposed a fuzzy based trust model. In our trust model, we determined four parameters for each peer to assess and to compare with other peers.

There are several techniques to use these parameters and aggregate them to provide a trust metric for trust evaluation. We create a fuzzy set with this parameter and move to a fuzzy space for trust evaluation. Fuzzy approach causes to affect many factors. This approach provides a framework to add other important factors. Fuzzy approach needs to a suitable algorithm to aggregate and compare peers. We use $D_{p,q}$-distance algorithm [23, 24] for aggregating. It is a real-value distance between the imprecise data. The analytical properties of $D_{p,q}$ depend on the first parameter p, while second parameter q characterize the subjective weight attribute to the sides of fuzzy number. If there are no reason to distinguish any of fuzzy number, $D_{p,q}$ is recommended.

# 3. THE TRUST MODEL

The trust relation is created by a resource request issued by one peer to other peers of the network in order to fulfill a requisite. As depicted in Figure 1, the trust relation includes three operators and three labeled edges [10]. In this figure, each trustor peers has a trust table. Each tuples of trust table is a fuzzy set. In the rest of this section, we first describe the trust parameters that used for trust evaluation. Then we present the aggregation of trust parameters to assess trustworthiness of each peer.

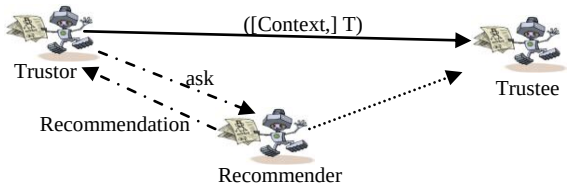


**Fig 1: Trust relation**

## 3.1 Trust Parameters

The peer relationships are established in pair wise interactions during which certain information or service is exchanged [1]. To help peers in evaluating the trustworthiness of a peer, the problem is to essentially determine a suitable trust mechanism or function that computes a trust value from information or input data that is relevant to the trust decision that is relevant to the trust decision a source peer is going to make [1].

In order to determine a suitable trust mechanism, we need to determine the trust parameters that can be used to assess the trust first. We identify four important parameters for such evaluation. They are satisfaction and unsatisfaction of trustor peers and recommender peers about a trustee peer. Each trustor peer to assess the trustworthiness of trustee peers, needs to create a fuzzy set from trust evaluation parameters. This fuzzy set is defined in equation (1):

$$\text{Trust\_Parameters}(o,e_i,R)=\{\text{UnSat}_{o,ei}, \text{Sat}_{o,ei}, \text{Sat}_{R,ei}, \text{UnSat}_{R,ei}\}, e_i \in E \quad (1)$$

Where, o is a trustor peer, E is a set of trustee peers; R is a set of recommender peers.

In the above equation, $\text{Sat}_{o,ei}$ denotes the amount of interactions that a trustor peer such as o fulfills its request by another trustee peer such as $e_i$, and wise versa $\text{UnSat}_{o,ei}$. $\text{Sat}_{R,ei}$ denotes the amount of interactions that recommender peers such as r fulfill their requests by trustee peer such as $e_i$ and $\text{UnSat}_{R,ei}$ is vice versa. In next section we use this fuzzy set to assess trustworthiness of peers and compare them.

## 3.2 Trust Model Architecture

In Figure 2 we show the structure of the proposed trust evaluation model. Each peer in this network has a Trust table. Trust table has a triple record that is shown in equation 2. In the initial stage, default values are equal to 0. There is no central database.

$$\text{Trust\_Table}(o)=\{\text{Peer, Sat, UnSat}\} \quad (2)$$

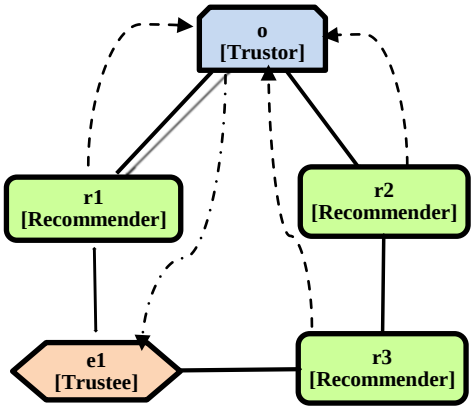


**Fig 2: Structure of trust evaluation mechanism**

**Table 1. A populated trust table**

| Trustee | Sat | UnSat |
|---|---|---|
| P2 | 5 | -2 |
| P4 | 2 | -4 |
| … | … | … |

For example, Table 1 shows a trust table for peer P1 that populated with some records. Peer P1 update its records according to the result of each transaction that P1 dose. Each trustor peer has the same trust table.

Suppose a trustor peer such as o wishes to find a trust measure for a trustee peer such as e, peer o should creates its fuzzy set that described in previous section. Peer o for creating fuzzy set need to calculate the values of each fuzzy set parameters. Calculations are performed in two steps. In first step, $\text{Sat}_{o,ei}$ and $\text{UnSat}_{o,ei}$ parameters are calculated locally. Peer o uses its trust table and gets these values. These values are computed as follows:

$$\text{Sat}_{o,ei} = (\text{ select Sat from trust table where peer}=e_i) \quad (3)$$

$$\text{UnSat}_{o,ei} = (\text{select UnSat from trust table where peer}=e_i) \quad (4)$$

In second step, we use the algorithm that presented in Figure 3 to compute values of $\text{Sat}_{R,ei}$ and $\text{UnSat}_{R,ei}$.

We suppose $\text{Sat}_{o,ei}$ and $\text{Sat}_{R,ei}$ have possitive value, and $\text{UnSat}_{o,ei}$ and $\text{UnSat}_{R,ei}$ have negative value. Finally, peer o can creates its fuzzy sets for each peer o and applies $D_{p,q}$ technique to aggregation trust parameters and creates trust metrics. These trust metrics can be used to assess trustworthiness of each peer $e_i$.

```
RSat=RUnSat=0;
For each Recommender peer r in Network Do
    RSat += (Select Sat From Trust_Table
              Where  Peer =e_i );
    RUnSat +=( Select UnSat From Trust_Table
              Where Peer = e_i );
End For;
```

**Fig 3: Calculating Sat and UnSat of recommender**

## 3.3 Trust Parameters Aggregation

In this Section, we use $D_{p,q}$-distance algorithm to aggregate trust parameters of each peers and create a suitable trust metric to compare and choice a peer. Let P denote the set of N peers in the network and o, E, R∈ P be peers in the network.

o is a trustor peer that request a resource, E is a set of peers that claim to provide requested resource, and R is a set of recommender peers.

Let $TP(o,e_i,R) = \{UnSat_{o,ei}, Sat_{o,ei}, Sat_{R,ei}, UnSat_{R,ei}\}$, $e_i \in E$ denote the fuzzy set that contains trust parameters. Let $TM(o,e_i)$ denote the trust metric computed from trust parameters. This trust metric is a measure to evaluate trustworthiness of peer $e_i$.

According to $D_{p,q}$ algorithm [23, 24], we need determine values of p and q. p is the analytical properties of this algorithm and we suppose that p=2. q is the weighting parameter, which is defined using following equation:

$$q = \frac{(Sat_{o,e_i} + Sat_{R,e_i})}{(Sat_{R,e_i} + UnSat_{R,e_i} + UnSat_{o,e_i} + Sat_{o,e_i})} \quad (5)$$

We present the template of trust metric equation as follow:

$TM(o,e_i) = D_{2,q}(TP_i(o,e_i,R), TP_{i+1}(o,e_{i+1},R))$, i in1 to n≤N, $e_i \in E$ (6)

In equation 6, $TP_i$ is a Trapezoidal Fuzzy number [25], therefore we redefine $TM(o,e_i)$ as follow:

$$\begin{aligned} TM^2(o,e_i) = \frac{(1-q)}{3}\{&(UnSat_{o,e_i} - UnSat_{o,e_{i+1}})^2 \\ &+ (Sat_{o,e_i} - Sat_{o,e_{i+1}})^2 \\ &+ (UnSat_{o,e_i} - UnSat_{o,e_i}) \\ &* (Sat_{o,e_i} - Sat_{o,e_{i+1}})\} \\ &+ \frac{q}{3}\{(UnSat_{R,e_i} - UnSat_{R,e_{i+1}})^2 \\ &+ (Sat_{R,e_i} - Sat_{R,e_{i+1}})^2 \\ &+ (UnSat_{R,e_i} - UnSat_{R,e_i}) \\ &* (Sat_{R,e_i} - Sat_{R,e_{i+1}})\} \end{aligned} \quad (7)$$

The trust metrics can be computed by the above equation for each trustee peer $e_i$. for comparison purpose, we can use the algorithm mentioned in Figure 4 to get more trustable peer. The value of Max denotes the index of more trustable peer. Peer o can choose peer $e_{max}$ to fulfill its request.

# 4. EXPERIMENTAL RESULT

In this section we describe the process of testing our algorithm. We test our algorithm on simulated P2P network implemented in Maple. We implement P2P network that a sample as such as network is shown in Figure 2.

```
Max=0;
For i=2  to n Do
    IF (TM(o,e_i) > TM(o, e_max)) Then
        Max=i;
    End IF
End For;
```

**Fig 4: Find more trust table peer**

In this network we have a trustor peer that requests a resource. There are two trustee peers as provider and two recommender peers.
The callout of the network shows that each peer maintains a small database that store trust table. We present trust tables of trustor and each recommender in Tables 2, 3, 4.

Table 2 shows the trustor peer o trust table. This table shows the results of experiences that trustor peer o have done with trustee peer $e_1$.Tables 3, 4 show the results of experiences that recommender peers have performed with trustee peer e1.

According to Figure 2, we use trust table of each peer to calculate TP(trust parameter fuzzy set).

In this network, recommender peers are $r_1$ and $r_2$, thus R= {$r_1$, $r_2$}. At first we use the following equation to calculate $TP_1(o,e_1,R)$:

$TP_1(o,e_1,R :: \{r_1\}) = (10, 12, 20, 22)$ (8)

Secondly, we use the following equation to calculate $TP_2(o,e_2,R)$:

$TP_2(o,e_2,R:: \{r_1\}) = (9, 11, 13, 17)$ (9)

In next step we calculate $TP_3(o,e_3,R)$:

$TP_3(o,e_3,R:: \{r_2\}) = (4, 4, 5, 9)$ (10)

Finally by applying $D_{p,q}$ algorithm, we create trust measure to compare peers. According to equation 5 calculation of q parameters are described in the following equation:

$$q_1 = \frac{12 + 20 + 11 + 13}{(12 + 20 + 11 + 13) + (10 + 22 + 9 + 17)} = 0.49$$

$q_2$=0.45, $q_3$=0.47 (11)

**Table 2. Trust table of peer o**

| Trustee | Sat | UnSat |
|---|---|---|
| e1 | 12 | 10 |
| e2 | 11 | 9 |
| e3 | 4 | 4 |

**Table 3. Trust table of peer $r_1$**

| Trustee | Sat | UnSat |
|---|---|---|
| e1 | 20 | 22 |
| e2 | 13 | 17 |

**Table 4. Trust table of peer $r_2$**

| Trustee | Sat | UnSat |
|---|---|---|
| e3 | 5 | 9 |

Each of these parameters is used to pair wise comparison of trustee peers. For example we use $q_1$ to compare $TP_1$ and $TP_2$.

To compare trustee peers, we compute $TM(o,e_i)$ as follows:

$TM_{1,2}(o,e_1)=D^2_{2,q1}(TP_1, TP_2)=18$
$TM_{2,3}(o,e_2)=D^2_{2,q1}(TP_2, TP_3)=49$
$TM_{1,3}(o,e_3)=D^2_{2,q1}(TP_1, TP_3)=119$

According to the values of TM, $TM_{1,3}$ has the maximum value thus trustor peer o selects $e_1$ to interact and fulfills its request.

## 5. CONCLUSION

We have proposed a Reputation-Based trust model for P2P networks. This trust model is discussed in a de-centralized P2P network. We used direct experience and recommendation of other peers to evaluate trustworthiness of each peers. This trust model has three massive characteristics. First, we used satisfaction and unsatisfaction experience of trustor and recommender peers. This causes to get a better judge about trustee peer. Second, we identified important common trust parameters and developed a fuzzy approach to them. By the nature of trust, since the trust is not simply a black and white notion, fuzzy approach and using a suitable algorithm for aggregation trust parameters are more important in trust evaluation mechanism. Third, we used a simple and performatic algorithm in the fuzzy space.

The proposed model in this paper can be used for agent-oriented environments. Each agent such as a peer in P2P network can use this algorithm and assess trustworthiness of other agents and select a reputable agent to interact. For future research, we consider multiple paths in trust evaluation and the trustworthiness of recommenders to detect malicious recommendation.

## 6. REFERENCES

[1] Xiong, L., and Liu, L. 2002. PeerTrust: A trust mechanism for an open peer-to-peer information system. Technical Report GIT-CC-02-29, Georgia Institute of Technology, College of Computing.

[2] Seti@home.http://setiathome.ssl.brekeley.edu.

[3] Genutella. http://www.genutella.com

[4] FreeNet. http://freenetProject.org.

[5] Chirita, P. A., Alex, P., Chirita, R., and Nejdl, W., and Schlosser, M., and Scurtu, O. 2004. Personalized Reputation Management in P2P Networks. In Proceedings of ISWC Workshop on Trust, Security, and Reputation on the Semantic Web.

[6] Kamvar, S. D., Schlosser, M. T. and H. G. Molina.2003. The Eigen Trust Algorithm for Reputation Management in P2P Networks. In Proceedings of the 12th International World Wide Web Conference(WWW 2003).

[7] VBS. Gnutella Worm.http://securityresponse.sym antec.com/avcenter/venc/data/vbs.gnutella.html.

[8] Artz, D., and Gil, Y. 2007. A survey of trust in computer science and the Semantic Web, Web Semantics: Science, Services and Agents on the World Wide Web, Vol. 5, No. 2,58-71.

[9] Rahimpour, B., and Matashborujerdi M. R. 2009. Using Hybrid Trust Model for Handling Inaccurate Resource, International Conference on Availability, Reliability and Security, CSS - ARES 2009-5-09-54.

[10] Shi, J., Bochmann, G., and Adams, C. 2004. A Trust Model with Statistical Foundation, IFIP vol. 173/2005, Springer, Toulouse, France, August 22-27, 145-158.

[11] Ray, I., and Chakraborty, S. 2004. A vector model of trust for developing trustworthy systems, In European Symposium on Research in Computer Security, pringer-Verlag, 260-275.

[12] Ray, I. Chakraborty, S., and Ray, U. 2005. A Trust Management System Based on a Vector Model of Trust.University of Colorado State, Springer.

[13] Ziegler, C., and Lausen, G. 2005. Propagation Models for Trust and Distrust in Social Networks, Information Systems Frontiers 7:4/5,337-358, Springer.

[14] Xiong, L., and Liu, L. 2003. A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities. Proceedings of the 4th ACM conference on Electronic commerce. ISBN:1-58113-679-X doi:10. 1145/779928. 779972.

[15] Zhao, H., and Li, X. 2009. Vector Trust: trust vector aggregation scheme for trust management in peer-to-peer networks. Computer Communications and Networks, ICCCN 2009.

[16] eBay, www.ebay.com.

[17] Xiong, L., and Liu, L. 2004. Peertrust: Supporting reputation-based trust in peer-to-peer communities, IEEE Transactions on knowledge and Data Engineering, vol. 16, no.7, 843–857.

[18] Kamvar, S. D., Schlosser, M. T. and H. G. Molina.2003. The eigentrust algorithm for reputation management in p2p networks, in Proceedings of the 12th International Conference on World Wide Web (WWW2003), Budapest, HUNGARY.

[19] Liang, Z., and Shi, W. 2005. Pet: A personalized trust model with reputation and risk evaluation for p2p resource sharing, in Proc.38th Ann. Hawaii Int'l Conf. System Sciences, I. C. Press, Ed.

[20] Song S., Hwang, K., and Zhou, R. 2005. Trusted p2p transactions with fuzzy reputation aggregation," IEEE Internet Computing, vol. 9, no. 6, 24–34.

[21] Lee, K. M., Hwang, K. S., Lee, J. H., and Kim, H.J. 2006. A Fuzzy Trust Model Using Multiple Evaluation Criteria. In Proceedings of FSKD. 961-969.

[22] Gambetta, D. 1990. Can We Trust Trust? In Trust: Making and Breaking Cooperative Relations. (Gambetta. D(ed.)). Basil Blackwell. Oxford.

[23] Sadeghpour-Gildeh, B., and Gien, D. 2001. La Distance-Dp,q et le Cofficient de Correlation enter deux variables aleatoires floues, Rencontres Francophomessur La Logigue Floue et ses Applications. LFA'01, 97-102.

[24] Bertoluzza, C., Corral, N., Salas. A. 1995. On a new class of distances between fuzzy numbers. Mathware and Soft Computing 2.

[25] Zadeh, L.1965.A Fuzzy Sets. Inform Control8, 338-353.

[26] Griffiths, N., Chao, K. M., and Younas. M. 2006. Fuzzy trust for peer-to-peer systems. In P2P Data and Knowledge Sharing Workshop (P2P/DAKS 2006), page To appear.