The ISC Int'l Journal of Information Security

July 2013, Volume 5, Number 2 (pp. 155–170)

http://www.isecure-journal.org

GTrust: A Group Based Trust Model

Mansooreh Ezhei [1,*] and Behrouz Tork Ladani [1]

[1] *Department of Computer Engineering, University of Isfahan, Isfahan, Iran*

ARTICLE INFO.

Article history:
Received: 13 March 2013
Revised: 4 September 2013
Accepted: 2 November 2013
Published Online: 20 March 2014

Keywords:
Trust, Group, Metagraph, GTrust.

ABSTRACT

Nowadays, the growth of virtual environments such as virtual organizations, social networks, and ubiquitous computing, have led to the adoption of trust concept. One of the methods of making trust in such environments is to use a long-term relationship with a trusted partner. The main problem of this kind of trust, which is based on personal experiences, is its limited domain. Moreover, both parties of such trust relationship will face big problems of collecting data and forming reasonable and reliable beliefs. Considering the concept of "group" in modeling trust is a way to overcome the above mentioned problems. Since, group-based trust is more suited with the nature of trust in new virtual environments. In this paper, a new trust model called "GTrust" is proposed in which trust is considered as a collective and shared feature of all group members. Therefore, group membership is used as the judgment criteria regarding a person's expected behavior and how he can be a trustee. GTrust is based on Metagraphs which are graphical data structures for representing a collection of directed set-to-set mappings. We show that by using GTrust, large trust spaces between unknown individuals can be shaped effectively. The proposed model not only offers a better description of human sense of trust when considering communities, but also provides the setting for evaluating the trust of individuals whom we do not know, and therefore provides an extended evaluation domain.

1 Introduction

Trust is an important yet complex relation among agents in social environments. With the growth of virtual environments such as virtual organizations, social networks, and ubiquitous computing, there is an increasing interest in bringing this concept into play. Therefore, modeling, evaluation and management of trust are of high importance. Trust plays important roles in the coalition formation, quality assessment and information credibility, and in determining how information flows between agents. Trust can be defined as the decision to rely on another party (i.e. person, group, or organization) under a condition of risk [1].

Experimental trust is a kind of trust that is acquired through continuous interaction with entities who have been known for a long time [2]. Most of the current trust management models are based on this viewpoint which normally uses directional graphs to describe the trust between persons. Even in models which try to infer indirect (transient) trust, only trust between persons is considered [3].

The main problem with experimental trust models

* Corresponding author.
Email addresses: m_ezhei@eng.ui.ac.ir (M. Ezhei), ladani@eng.ui.ac.ir (B. Tork Ladani)
ISSN: 2008-2045

is their limited domain. In virtual environments, we are normally faced with a huge number of users who engage in activity in big or small groups. Also, the prominent features of these environments are mobility and cooperation, so it may be unreasonable to rely on the old strategy of making trust based on personal experiences, since it results in the probability of losing many potentially profitable mutual interactions. Another problem with experimental trust is that the behavior of the trustee should be sufficiently clear and the trustor should be in a position to be able to monitor it for a long time. In any case, both parties of the relation are faced with big problems in collecting data and forming reasonable and reliable beliefs [2].

On the other hand, if people trust only on the basis of their personal experiences or that of their acquaintance, many kinds of business and partnerships would be impossible. It is indicated by many examples in which people test their chance against strangers. Hence, in environments in which there is no opportunity for either long term interaction or the expansion of personal history between parties of a relation -due to high dynamicity, or there is no information about the reputation of a certain entity- heuristic methods are used.

These methods include relying on groups as the trust intermediate [4]. Taking groups into account is not only a normal way of stating casual trust relations, but also is a means to overcome the above mentioned problems. In other words, if groups are designed perfectly, they can provide the basis for trust in people with whom we never have been familiar [5]. Such a model helps in the creation of trust between unacquainted institutions easily and with less communication and calculation overhead. Also, this model can be used in procuring trust in large environments.

In this paper we introduce a new model for evaluating trust in which trust is recognized as a common feature among groups. We call the proposed model "GTrust". In this model, group membership is regarded as the judgment criteria for the possible behavior of a person and the way he can be considered as a trustee. Groups provide the transition of trust from persons with whom we have never had contact. For example, two persons who have never known each other can gain mutual trust through belonging to a group or existence of (direct or indirect) relations between their groups. Also, trust between persons may be the result of the trust creation among their corresponding groups.

In GTrust, not only different possible kinds of trust relations between persons and groups are considered, but also the transition of trust from group to person and vice versa is introduced. We use metagraph [6] - a graphical data structure for representing a collection of directed set-to-set mappings - for representation and calculation of trust relations. Trust propagation is then modeled using operations on the paths of this metagraph. Our simulations shows that using the proposed model, precision and performance of trust calculation is enhanced especially when we are faced with unknown persons in a social environment.

In the rest of this paper, first in Section 2 a brief review and analysis on the related works are presented. Then after a short review of concepts and definitions of metagraph in Section 3, we have an analysis on trust relationships in the context of group in Section 4. After that in Section 5, we describe the basic properties of the proposed model, and in Section 6 two extended version of GTrust i.e. fuzzy GTrust and contextual GTrust are introduced. In Section 7 we discuss the properties and potentials of GTrust. Finally, conclusions will be drawn in Section 8.

2 Related Work

Information on past mutual interactions can be used to predict an agent's future behavior, but as mentioned in Section 1, there are some problems with models using such information such as limitation of the domain, so, group-based trust models are recommended. In this section we try to review and analyze the related works in this regard.

Yasutomi *et al.* [7] proposed a group-based reputation aggregation method in peer to peer networks called GRAT. GRAT calculates global reputation scores by dividing all peers into groups and each peer exchanges reputation data among peers that belong to the same group. In this way, even if the number of peers increases in the network, it takes shorter time to calculate global reputation scores. In another similar work, if the trustor does not know the target node, it aggregates feedbacks from its co-group to derive the value of trust to target node [8]. Such methods only use the concept of group to restrict information exchange among nodes and hence to reduce the communication loads of trust computation.

In StereoTrust [9], a user has to group other agents via forming stereotypes using his previous transactions with other agents. In this way, when facing a new agent (a stranger), the user estimates the agent's trust using the stereotypes of the groups which the new agent belongs to. In the Secgrid model [3], a hyper graph is used to model group trust. In this model, users in the same strongly connected component form a new group (hyperedge). Members within a group have the minimal level of trust that is represented by the hyperedge label. It is important to note that the

problem in the above two methods is cluster seeking to determine the potential group in a network based on the density of linkage, or similarity between nodes which is different from what we consider here. In our approach we assume that groups of interest have already been explicitly identified. In the following, we focus on models which are based on this assumption.

CMGTGR [10] calculates group trust and group reputation based on individual trust and the trustor's direct observation. In Dai, Wang *et al.* [11] approach, the trust between group and members is calculated using the Bayesian method. A similar work has been done using subjective logic [12]. GTMS [13] is another group-based trust management scheme for clustered wireless sensor networks which works on two topologies: intra-group topology, where the distributed trust management approach is used, and inter-group topology,where the centralized trust management approach is adopted. GTMS helps reduce drastically the cost associated with the trust evaluation of distant nodes. Zhang & Chen [14] proposed a method for trust calculation for members within a group based on direct experience and trust calculation for members from different groups based on the relationship between their groups. Ravichrandan *et al.* [15], modeled inter-group and intra-group trust using graphs. Interaction among members within a group is formed based on values of intra-group trust and interaction among members out of a group is formed based on values of extra-group trust. Gummadi *et al.* [16] used the same approach to estimate trust for peer-to-peer access control. Bistarelli *et al.* [17], introduced the notion of multitrust and assert that "the relationship of trust concerns one trustor and multiple trustees in a correlated way." The authors use and/or graph to display multitrust.

None of the above models consider all kinds of group trust relations as well as the trust transferability between groups and members (i.e. the mutual relationship between trust in interpersonal and intergroup levels) comprehensively and in a coherent way. Also, the simultaneous representation of person and group relations through standard graphs may be impossible, since a graph cannot display a relation in which there exists more than one element in the input and output of a relation. In addition, hypergraph cannot distinguish between input and output elements. Another method, i.e. and/or graph also suffers from high complexity of representation.

It is essential to use a method for a simple yet complete representation of directional relations between two sets (as well as their members) and to provide their algebraic analysis. In the proposed model in this paper, the metagraph [6] is used to represent trust relations in a group-based trust model. We will briefly explain the concepts of metagraph in the following Section.

3 Metagraph

In 1992 Basu and Blanning [6], introduced the concept of metagraph. Metagraph is a graphical hierarchical data structure for defining directional relationships between sets of (one or more) elements. It has all the properties of graphs. In weighted metagraph, numerical labels are added to the edges and each label assigns a weight to the corresponding edge.

Definition 1. The generating set of a metagraph is the set of elements $X = \{x_1, x_2, \ldots, x_n\}$, which represents variables of interest occurring in the edges of the metagraph.

Definition 2. An edge e in a metagraph is a pair $e{=}<V_e, W_e>\in E$ (where E is the set of edges) consisting of an invertex $V_e \subset X$ and an outvertex $W_e \subset X$, each of which may contain any number of elements. The different elements in the invertex (outvertex) are co-inputs (co-outputs) of each other.

Definition 3. A metagraph $S = <X, E>$ is then a graphical construct specified by its generating set X and a set of edges E defined on the generating set.

Definition 4. The adjacency matrix A of a metagraph is a square matrix with one row and one column for each element in the generating set X. The ij'th element of A, denoted as a_{ij} , is a set of triplets, one for each edge e connecting x_i to x_j. Each triplet is of the form $<CIe, COe, e>$, in which CIe is the co-input of x_i in e and COe is the co-output of x_j in e.

Definition 5. A simple path $h(x, y)$ from an element x to an element y is a sequence of edges $<e_1, e_2, \ldots, e_n>$ such that:

$x \in invertex(e_1)$,
$y \in outvertex(e_n)$, and
for all e_i, $i = 1, \ldots,$ *for all* e_i, $i = 1, \ldots$, *n-1*,
$outvertex(e_i) \cap invertex(e_{i+1}) \neq \varnothing$.

Definition 6. Conditional metagraph is a metagraph including propositions. Each edge may contain zero, one, or more propositions, and each proposition may appear in one or more edges. If a proposition appears in an edge, it must be true for the edge to be used in a path.

Definition 7. Given a conditional metagraph $S = <X_v \cup X_p, E>$, a set of propositions $P \subseteq Xp$ that are known to be true and a set of propositions $Q \subseteq Xp$ that are known to be false, define a *context K(P,Q,S)* as a conditional metagraph derived from S as follows:

1. For any edge $e \in E$ containing a proposition $p \in P$ simplify the edge by deleting p; if the resulting

edge has a null in- or out-vertex, delete the edge;
2. For any edge $e \in E$ containing a proposition $q \in Q$ in either vertex, delete the edge (only the edge and q are deleted, not the other elements in the edge's vertices).

Example 1. Consider metagraph S = <X, E> in Figure 1 . The generating set is X = $\{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$ and the set of edges is $E = \{e_1, e_2, e_3, e_4\}$ as follows:

$E = \{<\{x_1\}, \{x_3,x_4\}>, <\{x_2\}, \{x_5\}>, <\{x_3, x_4\}, \{x_6, x_7\}>, <\{x_4,x_5\}, \{x_6\}> \}$ Where, $e_1 = <\{x_1\}, \{x_3,x_4\}>$, $e_2 =<\{x_2\}, \{x_5\}>$, $e_3 = <\{x_3, x_4\}, \{x_6, x_7\}>$, $e_4 = <\{x_4,x_5\}, \{x_6\}>$

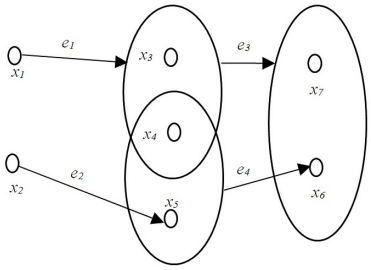


Figure 1. A metagraph example

In-vertex is a function with one argument which finds out the internal vertices from a given set. For example:

$$\text{In-vertex } (<\{x_3, x_4\}, \{x_6, x_7\}>) = \{x_3, x_4\}$$

Another function is out-vertex with one argument which finds out the out vertices from the given set. For example:

$$\text{Out-vertex } (<\{x_3, x_4\}, \{x_6, x_7\}>) = \{x_6, x_7\}$$

The co-input and co-output operations are two other functions of metagraph. Each of them has two arguments. For example:

$$\text{Co-input}(\{x_3, <\{x_3, x_4\}, \{x_6, x_7\}>\}) = \{x_4\}$$

$$\text{Co-output } (\{x_6, <\{x_3, x_4\}, \{x_6, x_7\}>\}) = \{x_7\}$$

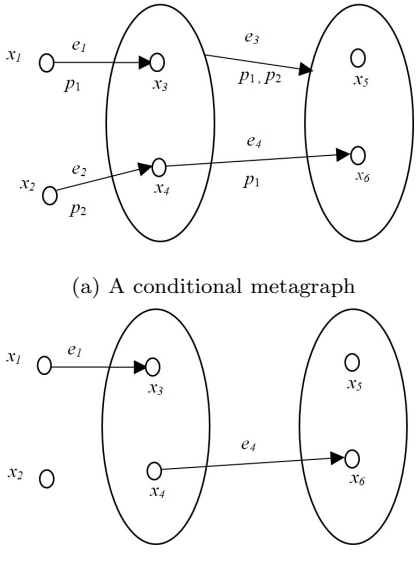
An example of a simple path is shown below.

$$h\ (x_1, x_6) = \{ <e_1, e_3> \}$$

$$h\ (x_2, x_6) = \{ <e_2, e_4> \}$$

The adjacency matrix of the trust metagraph in Figure 1 is shown in Table 1.

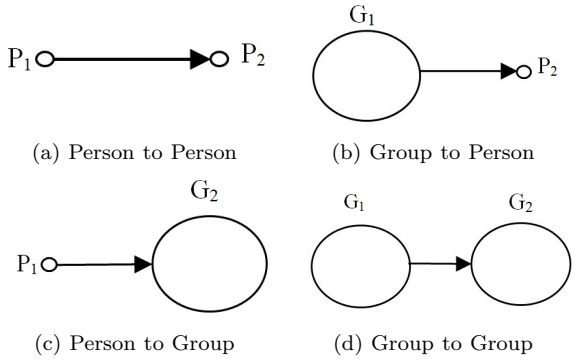
An example of a context metagraph is shown in Figure 2. Considering the conditional metagraph S in Figure 2a, K ($\{p_1\}$, $\{p_2\}$, S) is the corresponding context metagraph in Figure 2b.



(a) A conditional metagraph

(b) The corresponding context metagraph

Figure 2. Conditional metagraph



(a) Person to Person

(b) Group to Person

(c) Person to Group

(d) Group to Group

Figure 3. Multilevel trust

4 Trust in Context of Group

In our group-based trust model, trust relations are considered in person and group levels. On this basis, trust relations are assumed as person-person, person-group, group-person, and group-group which are shown in Figure 3. In each case the first element is the trustor and the second, is trustee.

Most of the current trust management models focus on the individual level. Trust calculation in these models is based on the transitive property of trust. At an individual level, two persons with little or no previous history or shared experiences can develop trust towards each other when they trust in a common third party. GTrust is based on another form of trust transfer. This form of trust transfer occurs when an individual that belongs to a group, transfers the trust, in that group to another member of the group whom, they have no previous history or shared experiences. Extension of this idea occurs as transmission of trust

Table 1. Adjacency Matrix of Metagraph in Figure 1

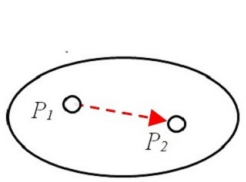
	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	$\emptyset$	$\emptyset$	$<\emptyset\ \{x_4\}, e_1>$	$<\emptyset\ , \{x_3\}, e_1>$	$\emptyset$	$\emptyset$	$\emptyset$
x_2	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$<\emptyset\ , \emptyset, e_2>$	$\emptyset$	$\emptyset$
x_3	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$<\{x_4\}\ , \{x_7\}, e_3>$	$<\{x_4\}\ , \{x_6\}, e_3>$
x_4	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$<\{x_5\}\ , \emptyset, e_4>$, $<\{x_3\}\ , \{x_7\}, e_3>$	$<\{x_3\}\ , \{x_6\}, e_3>$
x_5	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$<\{x_4\}\ , \emptyset, e_4>$	$\emptyset$
x_6	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
x_7	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

in external group (that the person does not belong to). Here trust transition occurs through detection of similarities among group members [18] Currall & Inkpen [1] stated that there exists a mutual relationship between trust in interpersonal and intergroup levels. In this way, interpersonal trust may lead to intergroup trust. Conversely, a background context of intergroup trust may result in interpersonal trust among group members. In the following we introduce an analysis of trust relationships between person and group. In this analysis, first the group is considered as an intermediate for trust between persons. Then, regarding the mutual relation between interpersonal and intergroup trusts, the person is considered as an intergroup trust intermediate.

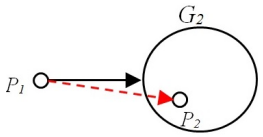
4.1 Group as Intermediate of Inter Personal Trust

As mentioned before, groups can be considered as trust intermediates to extend trust relationships. Well-designed groups can result in trust of unknown person. For example, two persons with little or no previous history or shared experiences can develop trust toward each other by simply belonging to the same group. In other words, a person can transfer his trust about a group to another member of that group even when he has no direct experience [18]. The logic behind this kind of trust making procedure is that: since I am familiar with or interested in the values of a certain group, I can trust every person belonging to that group [2].

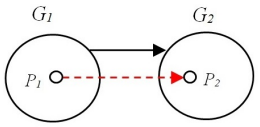
Different kinds of trust transition from group to person are presented in Figure 4. The continuous lines represent the person's primary trust relationships and the broken lines represent secondary trust relationships. For example, in Figure 4b the person P_1 wants to evaluate his trust on person P_2. P_2 belongs to group G. Assuming a primary trust between P_1 and G; P_1 can transmit his trust of group G to P_2.



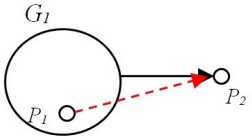
(a) Transition of trust within a group.



(b) Transition of trust to an external group into trust to members of that group.



(c) Transition of intergroup trust into inter personal group member trust.



(d) Transition of group trust to an external person into trust of members of the group to the external person.

Figure 4. Group as intermediate of interpersonal trust.

4.2 Person as Intermediate of Intergroup Trust

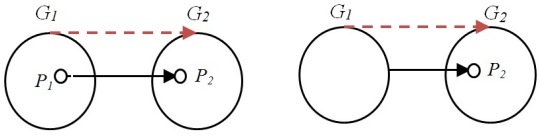
There is a mutual relationship between trust in interpersonal and intergroup levels. As a group can provide interpersonal trust, a person can also provide intergroup trust. Different kinds of trust transition from person to group are demonstrated in Figure 5.

5 GTRUST: Basic Model

In this section the basic properties of the GTrust model, including representation of trust relations as well as trust calculation and propagation in group context are introduced.

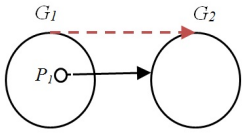
5.1 Representation of Trust Relations

Current trust management systems generally use directed graphs for describing trust among persons. However a directed graph is not sufficient to represent trust relationships when we consider the concept of



(a) Transition of inter personal group members trust into inter group trust.

(b) Transition of group trust to an external person into inter group trust.



(c) Transition of person trust to an external group into inter group trust.

Figure 5. Person as intermediate of group trust.

group. We propose the GTrust model which uses the metagraph for modeling group-based trust.

Trust concepts in GTrust are considered as follows:

(1) Trust values among groups are represented using weighted metagraph,
(2) Generating set X represents persons,
(3) Edges between two groups indicate the existence of trust between them. For example the edge $e = <V_e, W_e> \in E$ represents the trust of group V_e toward group W_e,
(4) The weight $w \in [0,1]$ of edge $e = <V_e, W_e> \in E$ is the numerical trust value of group V_e toward group W_e.

As an example, consider the metagraph S = <X, E< in Figure 6. The generating set is X = $\{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$ and the set of edges is $E = \{e_1, e_2, e_3, e_4\}$ as follows:

$E = \{<\{x_1, x_2\}, \{x_4\}>, <\{x_2, x_3\}, \{x_5\}>, <\{x_4, x_5\}, \{x_6, x_7\}>, <\{x_5\}, \{x_7\}>\}$

Where,

$e_1 = <\{x_1, x_2\}, \{x_4\}>$, $e_2 = <\{x_2, x_3\}, \{x_5\}>$, $e_3 = <\{x_4, x_5\}, \{x_6, x_7\}>$, $e_4 = <\{x_5\}, \{x_7\}>$

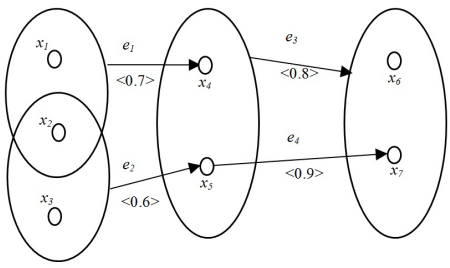


Figure 6. A trust metagraph example.

The edge e_1 between groups G_1 (i.e. $\{x_1, x_2\}$) and G_2 (i.e. $\{x_4\}$) is labeled< 0.7>. It shows that there exists a trust relationship between group G_1 and group G_2 and the trust value of group G_1 toward group $G_2$is 0.7.

5.2 Computation of Trust Values

The goal of this section is to provide a mechanism for deriving trusts values from one person to another when there is no direct relationship between them but they belong to the same group or there exists trust relationship between their groups. It means that, for example if x_i belongs to group G_1 and x_j belongs to group G_2 and there is a trust relationship between $G_1$and G_2, then x_i will trust x_j as a result of the existing trust between G_1 and G_2. In this case, the trust values between two persons can be simply considered as the trust value between their groups.

These issues are well consistent with the definition of the adjacency matrix in the metagraph. Hence, we will use this concept to develop the above mentioned idea.

As an example, consider Figure 7. G_1 includes element x_i and G_2 includes element x_j, edge e indicates the trust of G_1 toward G_2. The trust value of element x_i toward element x_j is considered as the weight of edge e in the adjacency matrix of the corresponding metagraph.

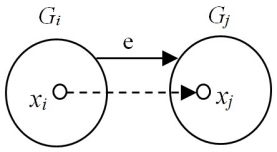


Figure 7. Trust value computation based on group membership.

The adjacency matrix of the trust metagraph in Figure 6 is shown in Table 2. In Figure 6, there are four groups: $\{x_1, x_2\}$, $\{x_2, x_3\}$, $\{x_4, x_5\}$, and $\{x_6, x_7\}$. If x_i and x_j belong to a single group, they will trust each other since they belong to the same group. Hence, in the adjacency matrix of the trust metagraph, the trust value between x_i and x_j is equal to 1. Here we simply consider the trust value of each person in his co-group to be 1.

Also the edge e_1 between nodes $\{x_1, x_2\}$ and $\{x_4\}$ in this metagraph is labeled by 0.7. It shows that $\{x_1, x_2\}$ trusts $\{x_4\}$ by the factor of 0.7. Therefore, each member in $\{x_1, x_2\}$ will trust x_4 by the factor of 0.7. Also, it is observed that x_5 trusts x_7 on basis of two paths. Both of these values are presented in adjacency matrix.

Table 2. GTrust adjacency matrix of the metageraph in Figure 6.

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	1	1	0	0.7	0	0	0
x_2	1	1	1	0.7	0.6	0	0
x_3	0	1	1	0	0.6	0	0
x_4	0	0	0	1	1	0.8	0.8
x_5	0	0	0	1	1	0.8	0.8,0.9
x_6	0	0	0	0	0	1	1
x_7	0	0	0	0	0	1	1

5.3 Trust Propagation

In Figure 8 element x_3 does not have any personal or group relationship with element x_8 and does not know the value of his trust toward x_8, but it is possible to calculate it through other groups or users. For example, he can ask x_7 how much his value of trust toward x_8 is. Alternatively, he can ask the question from x_4 who in turn may ask x_6. The person x_6 may find the amount of trust toward x_8 using the value of trust between $\{x_6, x_7\}$ and $\{x_8\}$. Such a path corresponds to a simple path in a directional metagraph. There are two simple paths $<e_3, e_5>$ and $<e_4, e_5>$ between x_3 and x_8. However x_3 can obtain the trust value of x_8 using two paths.

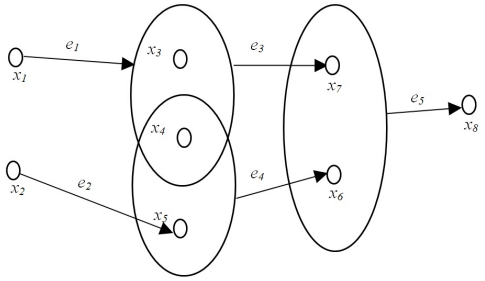


Figure 8. Trust path examples.

For each path like $x_1 x_2 \ldots x_n$ in Figure 9 an estimated trust between x_1 and x_n is calculated by the following propagation algorithm:

$$t_{x_1 x_n} = t_{x_1 \tilde{x}_2} \times t_{x_2 x_3} \times \cdots \times t_{x_{n-1} x_n} \qquad (1)$$

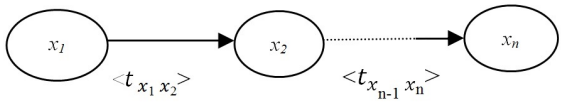


Figure 9. Trust propagation.

5.4 Trust Aggregation

To find the trust value when there are multipath ways of propagation, we can make use of various methods:

(1) **Strongest path method:** in this method, all paths between $x_3$and x_8 can be found and the highest trust value existing among them will be considered as the result. This method has a main drawback: It may be too optimistic sometimes. The vote of the nodes with the highest trust values is not necessarily, always true.

(2) **Weakest path method:** in this method, the minimal amount of trust value between different paths is calculated and returned as the trust between two persons. This method has the drawback of the previous method since it considers pessimistic votes.

(3) **Average path method:** in this method, the amount of trust from all possible paths between two nodes is calculated and their average is returned as output. This method does not have previous method's problems; however, finding all possible paths between two nodes in such a metagraph is time consuming.

Consider the metagraph in Figure 6. As an example, the propagated trust matrix using the strongest path method is shown in Table 3.

Table 3. GTrust adjacency matrix of Figure 6 after trust aggregation.

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	1	1	1	0.7	0.7	0.63	0.63
x_2	1	1	1	0.7	0.7	0.63	0.63
x_3	1	1	1	0.7	0.7	0.63	0.63
x_4	0	0	0	1	1	0.9	0.9
x_5	0	0	0	1	1	0.9	0.9
x_6	0	0	0	0	0	1	1
x_7	0	0	0	0	0	1	1

In Figure 6, element x_1 does not have any personal or group relation with element x_7 and does not know the amount of his trust value towards x_7. However, he can obtain this value through the paths $<e_1, e_3>$, or $<e_1, e_4>$, or $<e_2, e_3>$, or $<e_2, e_4>$. The trust values in these paths are 0.56, 0.63, 0.48, and 0.54 respectively. So, the strongest and the highest value (0.63) is chosen. Note that the above three methods can be simply implemented by using *max*, *min* or *average* functions.

6 GTRUST: Extended Models

In this section we extend the previous basic model to capture more advanced properties of trust relations in group context.

6.1 Fuzzy-GTrust

Until now it was supposed that people in a group simply have the same fixation to the group. However, since persons might possess different positions within a group, they will have different membership degrees. The higher a degree in the group, the more likely the behavior of the person will be based on the standards and norms of the group. Membership degree represents the behavior of the person in the group. Therefore, in order to calculate the trust value of a person based on group membership, these criteria should also be considered, so, the membership degree is defined as the following function:

$$\mu : (Person, Group, Motivation, Attraction, Position) \rightarrow [0, 1]$$

Person and Group are the given person and group. Motivation shows the level of the person's participation in group interactions and responsibilities. Attraction represents the amount of the person's connection to the group. A person with low attraction value may easily leave the group. Position represents the power and influence of the person in the group which is dependent on social relations created in the group by that person as well as the amount of his capability and expertise in performing tasks in group [19]. μ is the function which returns the numerical value of the person's membership degree in the group based on the these parameters.

In order to use the membership degree for the calculation of trust, first it should be represented in an adjacency matrix and then a method should be applied to calculate the trust toward each element based on its group and his corresponding membership degree. In the following, each item is explained in more details.

Representation of Fuzzy Trust Relations In the basic GTrust model, membership degree of persons in the same group is supposed to be 1. It was shown however that, in real world, not only persons have different membership degrees in a group (ranging from 0 to 1), but also the trust value is estimated with different confidence. In this way, metagraph vertexes and edges will have a fuzzy representation (which is called fuzzy metagraph). The fuzzy metagraph, which is a generalization of metagraph is defined as follows [20]:

Definition 8. Consider a finite set $X = \{x_1, x_2, \ldots, x_n\}$. A fuzzy metagraph is a triple $<X, \widetilde{X}, \widetilde{E}>$ in which $\widetilde{X}$ is a fuzzy set on X and $\widetilde{E}$ is a fuzzy edge set. A fuzzy set $\widetilde{X}$ on X is completely characterized by its membership function μ: $X \rightarrow [0, 1]$. For each $x \in X$, $\mu(x)$ illustrates the truth value of the statement of "x belongs to $\widetilde{X}$". A fuzzy edge set $\widetilde{E}$ is defined as a function $\rho : E \rightarrow [0, 1]$, the membership value of an edge is also called certainty factor (CF) of the edge. For simplicity, assign $\widetilde{x}_i$ denoting $(x_i, \mu(x_i))$ and $\widetilde{e}$ denoting $(\widetilde{e}, CF_e)$, i.e.,$(\widetilde{e}, \rho(e))$.

Trust concept in Fuzzy-GTrust are considered as follows:

(1) Trust values among groups are represented using fuzzy metagraph
(2) Fuzzy set $\widetilde{X}$ represents persons and their membership degrees in their corresponding groups.
(3) Edges between two groups indicate existence of trust between them. For example the edge $\widetilde{e} = <\widetilde{V}_e, \widetilde{W}_e> \in \widetilde{E}$ represents the trust of the group $\widetilde{V}_e \subset \widetilde{X}$ to the group $\widetilde{W}_e \subset \widetilde{X}$.
(4) The label of edge $\widetilde{e} = <\widetilde{V}_e, \widetilde{W}_e> \in \widetilde{E}$ is a couple of values <t; c>: the first component is the trust value of group $\widetilde{V}_e$ to group $\widetilde{W}_e$, while the second component is the quality of the trust value assignment (i.e. a confidence value), both of these components are in the range [0, 1].
(5) A high trust value means that the trustee have gained a good feedback, whereas a confidence value close to 1 indicates that the trustor estimates the correlated trust value with precision.

As an example, consider the metagraph $S = < X, \widetilde{X}, \widetilde{E} >$ in Figure 10. The generator set is $X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$ and the fuzzy set is $\widetilde{X}$ as follows:

$$\widetilde{X} = \{\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4, \tilde{x}_5, \tilde{x}_6, \tilde{x}_7\}$$

Where,

$\tilde{x}_1 = (x_1, \mu(x_1))$, $\tilde{x}_2 = (x_2, \mu(x_2))$, ..., $\tilde{x}_7 = (x_7, \mu(x_7))$ and

$G_1 = \{x_1, x_2\}$, $\mu(x_1) = 0.8$, $\mu(x_2) = 0.9$

$G_2 = \{x_2, x_3\}$, $\mu(x_2) = 0.9$, $\mu(x_3) = 0.7$

$G_3 = \{x_4, x_5\}$, $\mu(x_4) = 0.8$, $\mu(x_5) = 0.6$

$G_4 = \{x_6, x_7\}$, $\mu(x_6) = 0.7$, $\mu(x_7) = 0.6$

and the set of edges is $\widetilde{E}$ as follows:

$$\widetilde{E} = \{\widetilde{e}_1, \widetilde{e}_2, \widetilde{e}_3, \widetilde{e}_4\}$$

Where,$\widetilde{e}_1 = <\{\tilde{x}_1, \tilde{x}_2\}, \{\tilde{x}_4\}>$, $\widetilde{e}_2 = <\{\tilde{x}_2, \tilde{x}_3\}, \{\tilde{x}_5\}>$, $\widetilde{e}_3 = <\{\tilde{x}_4, \tilde{x}_5\}, \{\tilde{x}_6, \tilde{x}_7\}>$, $\widetilde{e}_4 = <\{\tilde{x}_5\}, \{\tilde{x}_7\}>$.

The edge $\widetilde{e}_1$ between groups G_1 (i.e. $\{\tilde{x}_1, \tilde{x}_2\}$) and G_2 (i.e. $\{\tilde{x}_4\}$) is labeled as $< 0.7;0.6>$. It shows that there exist a trust relationship between group G_1 and

group G_2 and the trust value of group G_1 to group $G_2$is 0.7, and it is estimated with precision 0.6.

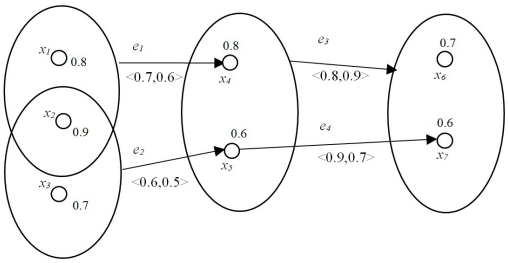


Figure 10. Fuzzy metagraph example

The corresponding trust and confidence value in the adjacency matrix are shown in Table 4.

Computation of Trust Values The trust calculation procedure for each element is similar to the procedure in Section 5.2. However, it is necessary to consider the membership degree of elements in trust calculation. The higher the membership degree of a person (i.e. the more fixations to goals and values of the group), the easier the trust will pass onto the members of the group.

Consider Figure 11 where $\mu(\mathrm{x_i})$ is the membership degree of x_i in group G_i and $\mu(\mathrm{x_j})$ is the membership degree of x_j in group G_j,and the amount of G_i's trust toward $G_j$equals $Trust(G_i, G_j)$, then to calculate the trust between x_i and x_j, based on their groups and their membership degree values, the following relation is used:

$$\mathrm{Trust}\ (\mathrm{x_i}\ ,\ \mathrm{x_j}\ )\ = \mu(\mathrm{x_i}) \times \mathrm{Trust}\ (\ \mathrm{G_i}\ ,\ \mathrm{G_j}\ ) \times \mu(\mathrm{x_j}) \tag{2}$$

In (2) the algebra multiplication has been used. The justification behind using the algebraic multiplication is that it is well suited with the nature of trust transitivity:

It is range protective: p, q∈[0,1] → p×q ∈[0,1]

It is commutative: p×q = q×p

It is associative: p×(q×r) = (p×q)×r

It is monotonic: p=q, r=s → p×r = q×s

It supports the boundary conditions: p×0 = 0, p×1= p

Although there are some other operators that satisfy the above properties, the multiplication operator is chosen, because not only it is simple, but also it well reflects the concepts of membership and trust value.

Trust Propagation and Aggregation The procedure of trust propagation and aggregation in fuzzy GTrust is shown in Figure 13. In this procedure, for each path like $\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n$ in Figure 12 an estimated trust between $\tilde{x}_1$ and $\tilde{x}_n$ is calculated by the following propagation formula:

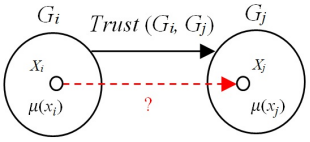


Figure 11. Group membership.

$$\begin{aligned}(t_{\tilde{x}_1\tilde{x}_n}, c_{\tilde{x}_1\tilde{x}_n}) = \\ (t_{\tilde{x}_1\tilde{x}_2} \times t_{\tilde{x}_2\tilde{x}_3} \times \cdots \times t_{\tilde{x}_{n-1}\tilde{x}_n}, \\ c_{\tilde{x}_1\tilde{x}_2} \times c_{\tilde{x}_2\tilde{x}_3} \times \cdots \times c_{\tilde{x}_{n-1}\tilde{x}_n})\end{aligned} \tag{3}$$

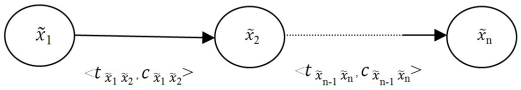


Figure 12. Trust propagation.

To find the trust value when there are multipath ways of propagation, we can make use of various methods:

(1) **Strongest path method**: Choose the path with the highest confidence value.
(2) **Average path method**: In this method the amount of trust from all possible paths between two nodes is calculated and their average is returned as output. Confidence value is computed as follow:

$$\mathbf{C}F_{combine}\ (\mathrm{CF1},\ \mathrm{CF2})\ =\ \mathrm{CF1} + \mathrm{CF2} \times (1 - \mathrm{CF1}) \tag{4}$$

This combined CF value has two desirable properties, coverage toward 1, but never quite reaches this value and incrementally add if there are multiple path between trustee and trustor.

6.2 Context-GTrust

Context has different definitions in different applications. Also, based on the intention of different people, it may carry varying implicational ranges. In this section, context is treated in terms of environmental conditions and trust aspects. We first discuss these two issues, and then we show how to represent context information in GTrust.

Environmental Conditions In many applications, we need to evaluate trust based on the environmental conditions of the system, including time, location, required security level, and cooperation/competition

Table 4. Fuzzy-Gtrust Adjacency Matrix of Figure 10.

	$\widetilde{x}_1$	$\widetilde{x}_2$	$\widetilde{x}_3$	$\widetilde{x}_4$	$\widetilde{x}_5$	$\widetilde{x}_6$	$\widetilde{x}_7$
$\widetilde{x}_1$	0	0	<0.7,0.6>	<0.7,0.6>	0	0	0
$\widetilde{x}_2$	0	0	0	0	<0.6,0.5>	0	0
$\widetilde{x}_{31}$	0	0	0	0	0	<0.8,0.9>	<0.8,0.9>
$\widetilde{x}_4$	0	0	0	0	0	<0.9,0.7>	0
$\widetilde{x}_5$	0	0	0	0	0	<0.9,0.7>	0
$\widetilde{x}_6$	0	0	0	0	0	0	0
$\widetilde{x}_7$	0	0	0	0	0	0	0

Algorithm Fuzzy GTrust
Input: A Fuzzy Metagraph adjacency matrix representing the fuzzy trust relationships between every two peers.
Output: Estimated Trust for pair x_i and x_j
Find all *simple paths* between the two users of x_i and x_j.
//Propapagation Stage
For each *path*
Calculate the trust value between users x_i and x_j using (3) .
Calculate the confidence value using (3) .

$$(t_{\tilde{x}_1\tilde{x}_n}, c_{\tilde{x}_1\tilde{x}_n}) = (t_{\tilde{x}_1\tilde{x}_2} \times t_{\tilde{x}_2\tilde{x}_3} \times \cdots \times t_{\tilde{x}_{n-1}\tilde{x}_n}, c_{\tilde{x}_1\tilde{x}_2} \times c_{\tilde{x}_2\tilde{x}_3} \times \cdots \times c_{\tilde{x}_{n-1}\tilde{x}_n})$$

//Aggregation Stage
Choose the path using either of the methods: Strongest path method or Average path method.

Figure 13. Fuzzy GTrust pseudo code.

levels. Sometimes if a relation is created in a specific time or location, then it would be more reliable.

For example the promise of a manager in an official time and place will be much more reliable than his promise made at other times and in other places [21]. Also, sometimes depending on the application goals and the required security level in the application, different methods of manipulating trust values are needed. For example, using other people's opinions and propagation of trust, may be allowed in one of the following ways:

(1) Unlimited: Using advice is allowed unrestrictedly. Due to the optimistic view of the environment, using positive advice about others is allowed
(2) Limited: Using other nodes' advices for calculation of trust is conservative and may even be discarded. For example, in propagation of trust, those edges should be used whose trust value exceeds a standard limit.

As yet another environmental condition affecting trust management we could refer to cooperation and competition amongst nodes. Depending on the amount of existing cooperation or competition among groups, transition of trust within personal and group levels may be blocked. For example, in the case of high competition among partner companies, they may have to avoid information disclosure to the outside. Such policies may prevent development of trust among managers of partner companies since concealing information from partners may result in suspicion toward the partner [1]. Therefore, the flow of trust in personal and group levels may be achieved in the following two ways:

(1) Inter group trust results in inter personal trust: this occurs when there is cooperation between partner groups.
(2) Inter group trust does not result in inter personal trust: this occurs when there is strong competition between partner groups.

Trust Aspects Trust between two institutions can be formed in different applications and fields. Each application as part of its context may use a special aspect of trust e.g. resources, advice, and friendship. Similarity between aspects has a key role in the easy transition of trust from one aspect to another. For example, moving from information exchange to advice exchange may be easier than moving from information exchange to resource exchanges [18]. Hence, the transition of trust from one aspect to another aspect of a trust relation will occur in the following two ways:

(1) Transferable: if aspects of a relation are close to each other, trust transition between these two aspects would be easier. For example, suppose

that person A has a great deal of trust on person B with respect to choosing a good director. An inferable conclusion is that A may also trust in B heavily regarding suggesting a good film.

(2) Non-transferable: when the distance between different aspects of a relation increases, it is more likely that the transition of trust between the two aspects will decreases. For example, trusting a person in the field of computer may not result in trusting him in the field of cooking.

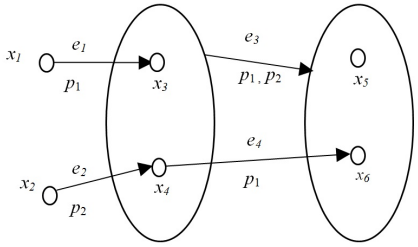
Context Representation Both concepts of environmental condition and trust aspects can be represented in the conditional metagraph (See Section 3 for its definition). The conditional metagraph includes propositions which are added to edges as a label and assign a condition to the corresponding edge.

Alternative contexts for a conditional metagraph can be specified using different proposition values. Let us consider P as the set of true propositions, Q as the set of false propositions and the remaining propositions as undetermined. In this case, a conditional metagraph can be simplified using such information in a way that retains only contextually valid edges.

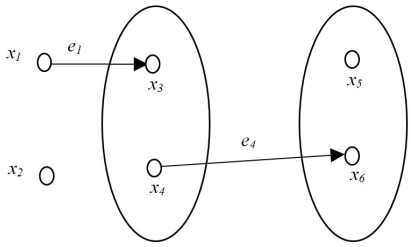
In particular, $K(P,Q,S)$ is the context representation of a conditional metagraph S with respect to P and Q; This is also a conditional metagraph where 1) any proposition in P is deleted and 2) any edge containing a proposition in Q is deleted. What results is a context metagraph which is a conditional metagraph since the propositions that are not determined will remain as propositions in the context. In relation to metagraphs, the context operation is a useful abstraction due to the fact that it avoids taking into consideration edges that cannot be used under the stated Q conditions.

An example of a context metagraph is shown in Figure 14. Considering the conditional metagraph S in Figure 14a, K ($\{p_1\}$, $\{p_2\}$, S) is the conditional metagraph in Figure 14b in which p_1= "Optimistic view towards the environment" and p_2= "There is cooperation between partner groups".

As we discussed in the previous section the flow of trust in personal and group levels can be achieved when there is cooperation between partner groups. p_2 is false, which means there is competition between these partner groups, the edges labeled with p_2 cannot be used in a path and are deleted. But, p_1 is true, which means there is an optimistic view towards the environment; therefore, using positive advice about others is allowed.



(a) A conditional metagraph



(b) The corresponding context metagraph

Figure 14. Conditional metagraph.

7 Evaluation

In this section we conduct an experimental analysis to show the applicability of GTrust for estimating interpersonal trust using group information.

We consider Epinion dataset which contains explicit groups. This dataset contains the crawled friendship network and the selected group membership information.

The basic statistics for this dataset are given in Table 5.

Table 5. Dataset Statistics.

	User	Group	Friendship pairs	Membership pairs
Epinion	131828	10312	736811	2042116

In Section 4, we stated that there exists a mutual relationship between trust in interpersonal and intergroup levels. This way, interpersonal trust may lead to intergroup trust. Conversely, a background context of intergroup trust may result in interpersonal trust among members of the group. We can evaluate the above theory with respect to the frequencies of the co-group among all friendship pairs.Table 6 gives the number and fraction of a person's friends that are in the same group with him. This analysis confirms that there exists a mutual relationship between trust in interpersonal and intergroup levels.

In Table 6, the tie that the membership and friendship links have been initiated is neglected. So we try to

Table 6. Friendship and the Co-Group.

	Count	Fraction
Friendship and the Co-Group	235488	0.32

find out how many friendship links have been created before membership links and how many after that.

First we consider the newly added friendships in our dataset for 12 months and the number of added friendships during each time interval. Based on our observation, the distribution of friendship link creation times is shown in Figure 15. The X axis is the time, and the Y axis is the number of newly added friendship links during each time interval.

Sometimes friendship links are created because two persons are both members of the same group [22]. We can evaluate the above theory with respect to the frequencies of the co-group among all newly added friendship pairs.Table 7 shows the percentage of the newly added friendships in which the involved pairs of users are both members of the same group.

This table illustrates that a high percentage of the new friendships involved pair of users are both members of the same group(s).

Sometimes friendship link already exists and a person joins a group because his friend is a member of that group [22]. To evaluate the above theory, we observe the newly added membership links. Figure 16 shows the distribution of the membership creation times. The X axis is the time, and the Y axis is the number of newly added membership links during each time interval.

Table 8 shows the percentage of users joining a group in which his friend(s) is a member of that group.

The above analyses confirm that there exists mutual relationship between trust in interpersonal and intergroup levels.

Here's another way to evaluate the model and we try to show the applicability of GTrust for estimating interpersonal trust using group information. We consider a subset of Epinion balanced dataset that 1000 node pairs are randomly chosen. Because there is no explicit trust network among groups in this dataset, we must compute the trust values between group pairs by considering the factors that influence on trust formation process between groups. One group trusts another group based on its history of interactions with individual members of that group [18]. Based on this fact, we compute the trust network between group pairs from a set of train set observations using rule induction algorithm [23].

We used the 10-fold cross-validation method for the evaluation of the proposed algorithms. In this technique, the train and test datasets are drawn from the same distribution. The desired trust edge value in test dataset is calculated through user-group membership of source and sink using the procedure in Figure 13 and then the calculated value is compared with the omitted value.

There are four possible outcomes for the algorithm:

(1) *True positive*: If there is trust relationships between two peers and the algorithm suggestion is 1.
(2) *False positive*: If there is no trust relationships between two peers and the algorithm suggestion is 1.
(3) *True negative*: If there is no trust relationships between two peers and the algorithm suggestion is 0.
(4) *False negative:* If there is trust relationships between two peers and the algorithm suggestion is 0.

Accuracy, *precision* and *recall* metrics are defined as follows:

When our method suggests trusting, the following parameters are considered:

$$Precision_{\mathbf{t}}=\frac{True\ positive}{True\ positive+False\ positive} \tag{5}$$

$$Recall_{\mathbf{t}}=\frac{True\ positive}{Positives} \tag{6}$$

Positives= the number of friends that we trust in reality.

When our method suggests no trust, the following parameters are considered:

$$Precision_{\mathbf{d}}=\frac{True\ negative}{True\ negative+False\ negative} \tag{7}$$

$$Recall_{\mathbf{d}}=\frac{True\ negative}{Negatives} \tag{8}$$

Negatives= the number of friends that we do not trust in reality.

The overall accuracy parameter is computed as follows:

$$Accuracy=\frac{True\ positive+True\ negative}{Positives+\ Negatives} \tag{9}$$

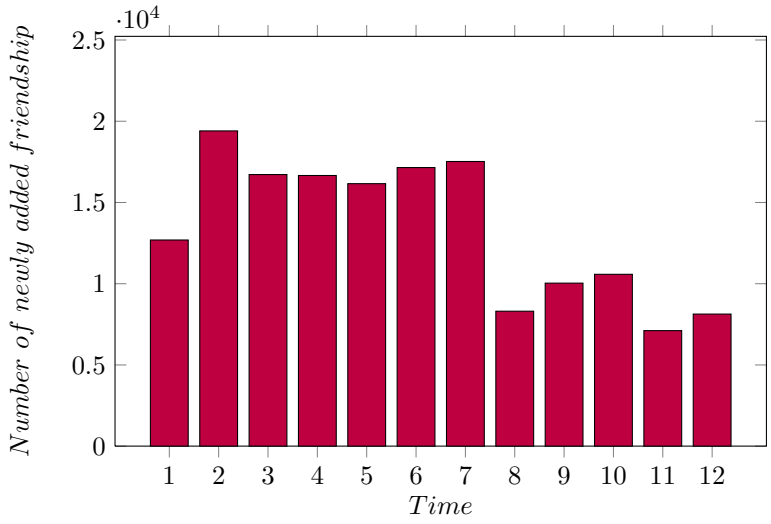


Figure 15. Distribution of friendship creation times.

Table 7. Percentage of new friendships with common Group(s).

Month	1	2	3	4	5	6	7	8	9	10	11	12	Avg
Percentage	67.76%	55.45%	55.39%	61.79%	63.51%	63.05%	62.97%	67.56%	68.51%	71.56%	62.81%	65.07%	63.79%

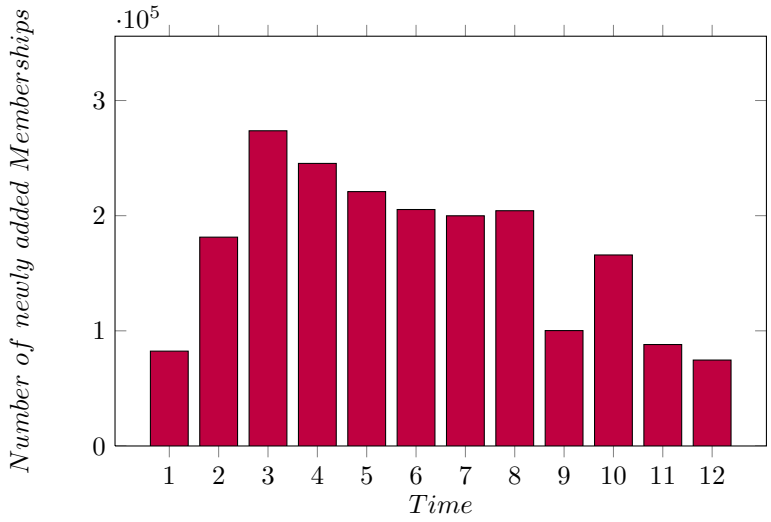


Figure 16. Distribution of membership creation times.

Table 8. Percentage of new Memberships with common Friend(s).

Month	1	2	3	4	5	6	7	8	9	10	11	12	Avg
Percentage	42.22%	49.61%	57.80%	59.97%	60.56%	60.81%	63.40%	65.40%	74.87%	72.07%	70.72%	71.56%	62.41%

However, there is a trade off between precision and recall. We use the following *Fscore* metric to measure the accuracy using recall and precision jointly for both trust and no-trust states:

$$Fscore = \frac{2 \times recall \times precision}{recall + precision} \qquad (10)$$

The evaluation metrics resulting from the implementation of propagation algorithm are shown in Table 9.

Figure 17 also shows the resulted ROC curves. ROC curve is a two-dimensional graph in which TP rate is plotted on the Y axis and FP rate is plotted on the X axis. TP rate and FP rate are defined as follows:

Table 9. Evaluation Metrics.

	$Recall_t$	$Precision_t$	$Fscore_t$	$Recall_d$	$Precision_d$	$Fscore_d$	$Accuracy$
Epinion	88.4%	90.84%	89.6%	97.3%	96.3%	96.79%	93.13%

$$TPrate = \frac{True\ positive}{Positives} \quad (11)$$

$$FPrate = \frac{False\ positive}{Negatives} \quad (12)$$

The ROC graph depicts the relative trade-off between benefits (*True positives*) and costs (*False positives*). Performance is measured by the area under the ROC curve (AUC). An area of 1 represents a perfect test; an area of 0.5 represents a worthless test. The result (AUC=0.963) shows that the proposed method has a good performance.

8 Conclusion

In reputation systems, the volume of states to be collected, preserved, and searched, is very high and hence such systems have serious problems with efficiency and data collection. The integration of personal behavior with group behavior allows measurable investigation and processing of reputation systems. Groups as intermediates and generalizer of trust provide the possibility of better trust making between persons unknown to each other. In this paper, GTrust as a new model based on group membership for solving the problem of trust in environments like virtual organizations and social networks was presented. In GTrust, the metagraph is used for the presentation of group trust and the trust value between two elements is calculated based on their group membership. In the case where there is no inter-group trust among two elements, trust value is calculated through trust propagation among users and groups.

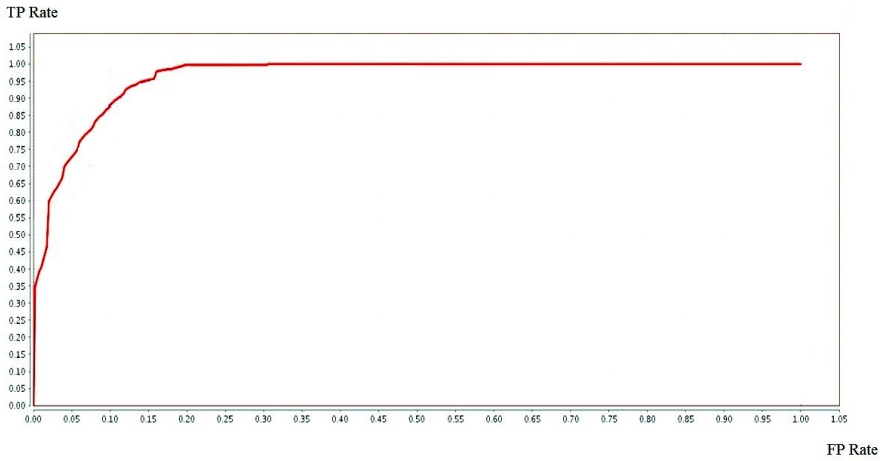


Figure 17. ROC curve

References

[1] S. C. Currall and A. C. Inkpen, "13 On the complexity of organizational trust: a multi-level co-evolutionary perspective and guidelines for future research," Handbook of trust research, p. 235, 2006.

[2] C. Offe, "How can we trust our fellow citizens?," Democracy and trust, pp. 42-87, 1999.

[3] R. Spanek, "SecGRID: model for maintaining trust in large-scale dynamic environments," International Journal of Grid and Utility Computing, vol. 1, pp. 146-158, 2009.

[4] M. Foddy and R. Dawes, "Group-based trust in social dilemmas," New Issues and Paradigms in Research on Social Dilemmas, pp. 57-71, 2008.

[5] M. Williams, "In whom we trust: Group membership as an affective context for trust development," Academy of Management Review, vol. 26, pp. 377-396, 2001.

[6] A. Basu and R. W. Blanning, Metagraphs and their applications: Springer, 2007.

[7] M. Yasutomi, Y. Mashimo, and H. Shigeno, "GRAT: Group Reputation Aggregation Trust for Unstructured Peer-to-Peer Networks," in Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference on, 2010, pp. 126-133.

[8] L. Wenzhi and L. Zhaobin, "Trust Assessment Model Based on Domain Group Collaboration," in 2009 First International Conference on Information Science and Engineering, 2009 pp. 3548-3551.

[9] X. Liu, A. Datta, K. Rzadca, and E. P. Lim, "Stereotrust: a group based personalized trust model," in Proceeding of the 18th ACM conference on Information and knowledge management, 2009, pp. 7-16.

[10] X. Tong and W. Zhang, "Group Trust and Group Reputation," in Fifth International Conference on Natural Computation, 2009, pp. 561-565.

[11] G. Dai, Y. Wang, Z. Jiang, and Y. Hou, "A Group Trust Model with Control Flow Constraint Based on Bayesian Method," in Computational Science and Optimization (CSO), 2010 Third International Joint Conference on, 2010, pp. 390-394.

[12] W. Yong and R. Xingtian, "A Group Trust Model with Control Flow Constraint Based on Subjective Logic," in Management and Service Science, 2009. MASS '09. International Conference on, 2009, pp. 1-6.

[13] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y. J. Song, "Group-based trust management scheme for clustered wireless sensor networks," Parallel and Distributed Systems, IEEE Transactions on, vol. 20, pp. 1698-1712, 2009.

[14] G. H. Zhang and Z. G. Chen, "A Robust Trust Model Based on Group for P2P Environments," Key Engineering Materials, vol. 439, pp. 98-103, 2010.

[15] A. Ravichandran and J. Yoon, "Trust management with delegation in grouped peer-to-peer communities," in Proceedings of the eleventh ACM symposium on Access control models and technologies, 2006, pp. 71-80.

[16] A. Gummadi and J. P. Yoon, "Modeling group trust for peer-to-peer access control," in Database and Expert Systems Applications, 2004. Proceedings. 15th International Workshop on, 2004, pp. 971-978.

[17] S. Bistarelli and F. Santini, "SCLP for trust propagation in small-world networks," Recent Advances in Constraints, pp. 32-46, 2008.

[18] B. McEvily, V. Perrone, and A. Zaheer, "Trust as an organizing principle," Organization Science, vol. 14, pp. 91-103, 2003.
[19] R. Prada and A. Paiva, "Believable groups of synthetic characters," in Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems, 2005, pp. 37-43.
[20] Z.-H. Tan, "Fuzzy metagraph and its combination with the indexing approach in rule-based systems," Knowledge and Data Engineering, IEEE Transactions on, vol. 18, pp. 829-841, 2006.
[21] E.Mokhtari, Z. Noorian, B. Tork Ladani, and M. Nematbakhsh. "A context-aware reputation-based model of trust for open multi-agent environments." Advances in Artificial Intelligence, pp. 301-312. Springer Berlin Heidelberg, 2011.
[22] M. McPherson, L. Smith-Lovin, and J. M. Cook, "Birds of a feather: homophily in social networks," Annual Review of Sociology, vol. 27, no. 1, pp. 415–444, 2001.
[23] J.Han., and M. Kamber, "Data Mining:Concepts and Techniques". Elsevier, San Francisco. 2006.

Mansooreh Ezhei received her B.S. and M.S. degrees in Computer Engineering from Isfahan University, Isfahan, Iran. Since September 2009, She has been a Ph.D. student in Software Engineering at Isfahan University, Isfahan, Iran. Her research interests include Security Economics, Trust and Game Theory.

Behrouz Tork Ladani received his B.S. in Software Engineering from University of Isfahan, Isfahan, Iran in 1996, and M.S. in Software Engineering from Amir-Kabir University of Technology, Tehran, Iran in 1998.He received his Ph.D. in Computer Engineering from Tarbiat-Modarres University, Tehran, Iran in 2005. He is currently an associate professor in Faculty of Computer and Information Technology Engineering and head of Information Technology Department in University of Isfahan. His research interests include Software Security, Cryptographic Protocols, Formal Specification and Verification, and Computational Trust. He is member of Iranian Society of Cryptology (ISC).