Group Formation with Neighbor Similarity Trust in P2P E-Commerce

Felix Musau, Guojun Wang*, Muhammad Bashir Abdullahi
School of Information Science and Engineering, Central South University
Changsha, Hunan Province, P. R. China, 410083
*Correspondence to: csgjwang@mail.csu.edu.cn

***Abstract*—The simplicity with which products and prices are compared in e-commerce brings an attractive option for many online merchants. The completion of online business transactions with the condition that one must provide personal information has always been an act that beckons hesitation. Most online traders are conscious of various threats and attacks such as credit card fraud, identity theft, spoofing, hacking, phishing, and other abuses, leading to low trust in transactions. P2P systems take place at the edge of the Internet. Peer communities are established dynamically with peers unknown to each other. In our proposed mechanism, peers form groups to ensure trust and security. Each group is established based on interest among peers. In this paper, we show how peers form groups, and select group leaders. A peer can belong to more than one up to *n* groups. The neighbor similarity behavior is shown by peers having common neighbors.**

***Keywords*-Group, similarity, P2P, e-commerce.**

I. Introduction

Compared with traditional networks, Peer-to-Peer (P2P) networks are vulnerable to various attacks due to their characteristics. P2P systems are targeted for information sharing, file storage, searching, and indexing, often using overlay networks. P2P e-commerce expands the scope of P2P systems by forming groups based on interest in their environments. There are many examples of electronic communities, e.g., Yahoo Groups and Google Groups. Applications like IP telephony, video/audio conferencing, online gaming, and file sharing are all increasingly getting organized as groups of peers. Others may exist as social groups such as political movements, professional organizations, and religious denominations. Information sharing, not only within a community, but also among communities, is a major driving force behind P2P networks.

In our scheme, we consider buyers and sellers in a business transaction where peers are individuals who use computers as peer devices. The trust information they exchange is on the products sales, discounts, new products, delivery methods, proof of quality of goods as ordered, etc. Cooperation among group members is a fundamental requirement due to anonymity, peer independence, high dynamics, and network conditions to effective security mechanism. The openness, anonymity, uncertainty, and dynamism of peers in P2P systems pose a challenge[1] in e-commerce which results in malicious nodes and free-riders to exist in a system, making it very difficult for e-commerce transactions.

Many e-commerce websites have been developed or are emerging, such as eBay, Taobao, Yahoo, and Amazon. Our work uses eBay as an example, which has a lot of shortcomings due to its centralized administration. We go further and suggest a decentralized system which addresses the issue of malicious peers. We use the idea of simple closed curves in a plane to show how peers can have same common interest similarity. Most existing trust models cannot fully address the issue of peers lying and having conspiracy. The major reason is lack of an effective cooperation mechanism inherently in P2P e-commerce. In e-commerce, people back up from meeting new strangers and buying new items that they did not know or try before [2]. Our work leverages the directed and undirected graph analogy-based approaches, and considers the common neighbor similarity interest in peer groups. The work brings accountability in uncertain infrastructure of P2P e-commerce.

The groups formed ensure that there is control of transactions as each group has its own administration policies. The Policies governing its members bring some identity which can make the peers accountable to any threats and attacks it has to others. In summary, there are two facts in previous researches. One is that many e-commerce systems rely on individual peers for doing transactions, which is very risky. The other one is that the peers always interact with new and anonymous peers in the dynamic environment.

Our contributions are threefold:

1) We present group formation of peers based on the interest to transact in an e-commerce environment.
2) Peers, which have common neighbors form a similarity group among the neighbors, which contributes to minimize maliciousness.
3) We present an easier way to search for products based on similar interest, as each group broadcasts the kind of goods or services it deals with.

The remainder of this paper is organized as follows: In the next sections, we describe the related work, preliminaries; group formation, overview of the proposed scheme, i.e., neighbor similarity trust, performance evaluation, and we conclude the paper in the last section.

II. Related Work

Group-based approach in e-commerce has been studied for some time, both in centralized and distributed trust models. A

978-0-7695-4600-1/11 $26.00 © 2011 IEEE
DOI 10.1109/TrustCom.2011.111

well-known group-based distributed trust model is the Eigen group trust model in P2P communities [3], which proposed an effective trust system built on top of a P2P group infrastructure.

Kamvar et al. [4] proposed a distributed trust model based on global reputation from local reputation, called EigenTrust. EigenTrust relies on good choice of some pretrusted peers, which are supposed to be trusted by all peers. The main problem of EigenTrust lies in the following aspects as pointed out in references [5]: 1) The precondition of iteration convergence is unreasonable; 2) It does not provide any punishment mechanism for bad behavior; 3) EigenTrust does not take into account user dynamics, and also does not consider the effect of credibility; and 4) EigenTrust does not bring security into consideration.

Tang et al. [6] proposed a grouping-based mechanism driven by reputation in P2P e-commerce (GDRep), in which peers are controlled by a central peer located in each group. The main problem of the mechanism is that: 1) There is no definite method in which a central peer is selected; 2) The method does not show how a peer can be punished after being dishonest in a transaction; and 3) There is no clear method on how peers communicate to each other, and how the data is stored in a group.

The GRBTrust model [7] assumes that one peer belongs to only one group, which ensures enough security as members can monitor activities of others. When a peer wants to cooperate with another peer, it first checks the reputation value of the other peer and then makes a decision. The method has a disadvantage as it restricts a peer to belong to only one group, which is often not the case in practice as proposed by our method.

Chung-Wei et al. [8] proposed trust between a trusting and trusted party must have a basis in some direct relationship. The relationship in question could be based on, or arise from a commercial, or social transaction, or through mere participation in common groups, or through an assessment of certain attributes that apply to each party. They propose that in real life, individuals and businesses give referrals and rely enormously on referrals to determine with whom to interact. The work failed to address the issue of interests in common groups.

Our work ensures security is enhanced by peers policing each other. If a peer misbehaves its reputation is affected and with time may reach a threshold level. We propose credibility in our work in addition to normalization for peers to be able to monitor each other in the group and report any malicious behaviors. In our proposed scheme each peer has a responsibility in administration in the group. Each group has a leader which selected, based on voting. In [4], it is assumed that a peer belongs to only one group. Our method advocates peers can belong to many groups but has a base group which is the first group it joined unless it has decided to change, which is out of scope of our work. Previous work does not address the idea of choosing the recommenders. Our work proposes that recommenders are initially selected from the neighbor peers who are well known to the concerned peer. Peers have an incentive as they can be able to identify potential business partners according to the trust levels.

III. Preliminaries

In this section, we give some definitions and explanations to form the basis of our scheme.

Definition 1 (*Neighborhood Graph*): A graph G is a tuple $\langle V, E\rangle$, where V is a set of vertices and E is a set of edges. Specifically, $V = \{v_1, v_2, ..., v_x\}$ represents the peers available, and $E = \{e_1, e_2, ..., e_y\}$ represents the edges among the peers. An edge is an ordered pair (v, z) of vertices, where v is called a trustor, and z is called a trustee. If vertex z is adjacent to vertex v, there is an edge (v, z) in E from v to z. Notice that if there is an edge (v, z) in E, then there is also an edge (z, v) in E. The neighborhood of a node v in a P2P e-commerce is $N(v) = \{z/(v, z) \in E\}$. Each node v maintains a set of identifiers of its neighbors in $N(v)$ in which each one is unique. Messages can be sent from a node v to a node z, provided that v knows the identifier of z. Any packet transmitted by a node is received by all its neighbors. Each edge in E, for example, from node a to node b, has two trust factors, namely trust value $t(a, b)$ and risk level $r(a, b)$, both of which take values from a real interval $(0, 1]$.

Definition 2 (*Nodes distribution*): A graph representing a P2P network should have a low degree, for each node in the graph to ensure a low maintenance cost, easy update in case of arrivals or departures of nodes, and changes in their positions. The nodes are distributed in a 2-dimensional Euclidean space represented by a set of points $V \subset \mathbb{R}^2$, which can also be extended to higher dimensions. Given any pair of nodes $u = (u_x, u_y)$, $v = (v_x, v_y) \in \mathbb{R}^2$, $\|uv\| = \sqrt{(u_x - v_x)^2 + (u_y - v_y)^2}$, denotes the Euclidean distance between u and v, sequence of nodes $s = (a_1, a_2, .., a_k)$ and any $\delta \geq 0$, $\|s\|^\delta = \sum_{i=1}^{k-1} \|a_i a_{i+1}\|^\delta$ denotes the δ-cost of s. The graph $G = (V, E)$ has a node sequence $s = (a_1, a_2, .., a_k)$ has a node sequence called a path in G if $(a_i a_{i+1}) \in E$, for all $1 \leq i < k$. For a directed graph $G = (V, E)$, and two nodes $a, b \in V$, the δ distance $d_G^\delta(a, b)$ of a and b in G is the maximum δ-cost $\|p\|^\delta$ over all paths p from u to v in G. If $\delta \geq 0$, then $d_G^\delta(a, b)$ gives the topological (hop) distance of u and v in G, and if $\delta = 1$, $d_G^\delta(a, b)$ gives the Euclidean distance of a and b in G. A trust value specifies the trust estimation that node i puts in node j. A similar concept can be seen in the real world, e.g., in Facebook, edges are friendships among people; in citation networks, nodes are papers, and edges are citations; in web graphs, nodes are webpages, and edges are hyperlinks.

IV. Group Formation

Keidar et al. [9] defined a group as a set of peers, or processes, while Ji et al. [10] defined a group as a community that is set up for a certain purpose. A group can be mathematically expressed as a set; it supports set operations, such as, union, intersection, subset, power set, Cartesian product, and complementation. So in a group $x \in (A \cup B)$, $\Leftrightarrow x \in A$ or $x \in B$ and $x \in (A \cap B)$, $\Leftrightarrow x \in A$ and $x \in B$.

A group has no empty set, and is dynamic in nature; it involves peers transacting e-commerce with varying interest changes. In our group formation model a peer, which intents to join a group looks for others with similar interest. In case it does not get any to join, it forms a new group. Each group introduces a group charter which specifies the rules each member has to follow. For group formation an incentive induced to each peer is the determinant for a peer to prefer to join. A peer will have an incentive that after joining the group which is tailored to identify trusted potential business partners. In addition, peers punish misbehaving ones by isolating them from the group.

After a peer joins a group, it gets a session key, and a key signed certificate, in which a signature can be validated with a verifiable secret sharing scheme (VSS). In a group, each peer has a receipt issued,which can be revoked if it voluntarily, or forcefully leaves. The joining and leaving of a group can be modeled as a continuous time stochastic process. The process is characterized by a rate parameterλ, also known as intensity, such that the number of events in time interval $(t, t + \tau]$ follows a poison distribution with associated parameter $\lambda\tau$. The relation is given as: $P(N(t + \tau) - N(t))$ = $\frac{e^{-\lambda\tau}(\lambda\tau)^k}{k!}$, k = 0, 1,$\cdots$ where $N(t + \tau) - N(t)$ is the number of events in time interval $(t, t + \tau]$. The process is characterized by its rate parameter λ, which is the expected number of events.

Algorithm: Group formation involves clustering the M peers into N groups. The basis is to use the distance between group leaders in existing groups to estimate the distance between two non-leader peers. We assume a peer will form or join a group which is near to it, if it trades on items of interest. The optimization criterion for group (G) formation is to minimize the n-Average Error as follows:

$$Min\frac{1}{M'}\sum_{i,j\in[1,..,n]}\sum_{x\in G_i,y\in G_j}|(x,\ y) - (S_i, S_j)|(x,\ y)^{-1}$$

A peer should join a group which has interest it requires and is near by checking the group leader to know the proximity. When a peer x joins a network, an algorithm is used to decide whether it needs to create a new group or join an existing group. When the leader leaves the system in dynamic P2P, the new leader performs the above process. At the bootstrapping stage, to avoid all peers joining at the same time, each peer sets an exponentially distributed delay timer and joins the system when its timer expires. The joining algortithm can be expressed as: $S^{'} = argmin_{S_j}\{x, S_j\} < (x, S_j)$, $j \in [1, .., n]$.

The peer x in G_i does not know the exact distances to other group leaders. It only knows (S_i, S_j) by intergroup communication. A group of peers have also challenges in that peers may become a liability to others. There are possible actions that can be lied about: providing service, not providing service, receiving service, and not receiving service. Falsely claiming to have provided service or not to have.

V. Overview of the Proposed Scheme

In this section, we propose interest similarity trust model in P2P e-commerce, and then the common neighbor similarity trust algorithm.

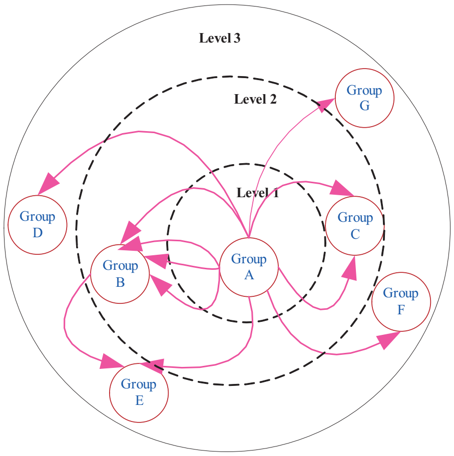

Fig. 1. Groups based on peer interest similarity.

A. Interest Similarity Trust Model

Peers organize themselves in groups which resemble sets. Between groups, there is intersection, which depends on similar interests. A peer can belong to different groups, represented as a Venn structure in a geometrical plane. Let $C = \{C_1, C_2, \ldots, C_n\}$ denote a family of n simple closed curves in the plane. The curves are required to finitely intersect. Let $X_i; i = 1, 2, \cdots, n$, be either the open bounded interior or the open unbounded exterior of the curve C_i. We say that C is a Venn structure if all of the $2n$ open regions $X_1 \cap X_2 \cap \cdots \cap X_n$ are non-empty and connected. If the connection condition is dropped, the diagram is called an independent family. The i-region in a Venn diagram is a connected region interior to two curves, which in our work represents groups overlapping.

Venn diagrams can be seen as a FISC [11]. A FISC is a family of Finitely Intersecting Simple closed curves in the plane representing groups, with the property that the intersection of the interiors of all the curves is not empty.

Theorem 1.1: In a FISC of n convex k-gons there are at most $\binom{n}{2}2k$ vertices. k-gon designate any convex polygon with at most k sides.

Proof: A pair of convex k-gons can intersect with each other at most $2k$ times; there are $\binom{n}{2}$ peers. A peer may have interest to transact with others in distant neighborhood as in Fig. 1. In our method, we consider two types of interest similarity groups.

- High intra-class interest similarity: It is cohesive in a group.
- Low inter-class interest similarity: It is distinctive between groups.

The work compares the similarity of two peers based on their common neighbors. The connection of nodes adopts the small world network phenomenon with a characteristic path length. At a random network, the aggregation coefficient from a node to another is high, but the path length is small.

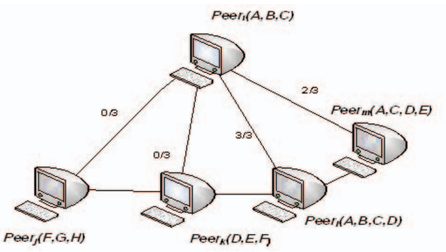

Fig. 2. Interest based neighborhood.

Levels are shown in Fig. 1, which have peers edged to their neighbors as per interest. The interest formed groups establish trust relationships by small world network to their distant peers in an optimal path. Trust, risk, and recommendations are propagated through paths. Before a search, peers should know their prerequisites: 1) local document vector; 2) neighbor peer set; 3) a specified TTL (Time to Live).

Our model perceives peers at long distances as having more opportunities to the group. Similarity is expressed in terms of reputation function, which is different for scaled, Boolean, categorical, ratio, and vector variables. Reputation based trust management can be recognized as an effective way for an open system to identify, avoid malicious nodes, protect the system from possible misuses, and abuses in a decentralized environment [12]. Groups and communities can be implicitly formed, i.e., if a peer in London declares an interest in wombats, and a peer in China also declares the same, the two peers become implicit, undiscovered community.

B. Similar Interest-based neighborhood

A peer can be able to know another peer with similar interest by studying the kind of goods they transact. Fig. 2 illustrates similarity interest, a $peer_i$ is looking for similar goods *A*, *B*, and *C* from $peer_j$ to $peer_m$. $peer_j$, has no goods matching the ones needed by $peer_i$. $peer_m$ has all the three goods. The goal is to identify peers of the same interest and group them together, or consider them as neighbors of the $peer_i$. If it has four neighbors, *j, k, l* and *m* then we say it has four edges, $i \to j, i \to k, i \to l$ and $i \to m$. Our edge network is based on selected neighbors. Following Liben-Nowell and Kleinberg [13], we define the attributes of the given pair of peers as the intersection of the sets of similar products. Probability of the edge between $peer_i$ and $peer_j$, $p_{pa}(i,j)\alpha|C_i||C_j|$; where C_i is the set of products of: $AA(i,j) = \sum_{k\in C_i\cap C_j}\frac{1}{\log(|C_k|)}$. The function is zero when two peers share no products, it creates a smooth distribution by interpolating between the normalized Adamic-Adar score, and a preferential attachment model.

C. Common Neighbor Similarity Trust

Similarity trust is derived from the similarity of the same set of neighbors based on interest in a pair of peers, i.e., p_i, and p_j. We use the Jaccard metric in which the similarity of $peer_i$ and $peer_j$ is defined as follows: $sim(p_i, p_j) = \frac{|p_i\cap p_j|}{|p_i\cup p_j|}$, where $|p_i \cup p_j| \neq 0$. If $sim(p_i, p_j)$ is not smaller than the similarity threshold *S*, then the interests of $peer_i$ and $peer_j$ are similar. The similarity relationship is symmetric, i.e., $sim(p_i, p_j) = sim(p_i, p_j)$. We can determine the dissimilarity between peers: $sim_\delta(p_i, p_j) = 1 - sim(p_i, p_j) = \frac{|p_i\cup p_j|-|p_i\cap p_j|}{|p_i\cup p_j|}$.

If N_i is the set of peer p_i's neighbors, and N_j is the set of peer p_j's neighbors. N_{ij} is the set of common neighbors of p_i and p_j assuming that the feedback is given by the peers which trade with that peer,hence $N_{ij} = p_i \cap p_j$, which are in the same or different groups defined as $N_{ij}' = p_i \cup p_j$. S_{ij} is the similarity between p_i's and p_j's trust value, about the same set of neighbors. It can be defined by the feedback of p_i's and p_j's trust value about the same neighbors. If *L*(*i, j*) represents p_i's local feedback about p_j, this also shows p_i's behavior in different transactions. Considering the set of common neighbors of p_i, and p_j: $N_{ij} = (H_1, H_2, \cdots, H_n)$. Assuming that *L*(*i, j*) represents p_i's feedback about p_j, and the p_i's report about p_j's behavior, which equates as the trust value, then: $\vec{Q}_i = \langle L(i,H_1), L(i,H_2), \cdots, L(i,H_n)\rangle$ is the p_i's trust vector about neighbors; $\vec{Q}_j = \langle L(j,H_1), L(j,H_2), \cdots, L(j,H_n)\rangle$ is p_j's trust vector[14].

We note the importance of credibility, and normalization of trust values in P2P e-commerce. A peer may award higher trust value to the friendly neighbors. Balanced normalization can be used to ensure that it is minimized or does not happen at all. This can be done by aggregating the trust value as discrete value between -1 and 1. We normalize by: $(nL)_{ij} = \frac{l_{ij}}{[TotalTransactions]_y^z}$, where *z* denotes upper bound of the time window, *y* denotes the lower bound, and time window can be denoted as *z* - *y* + 1. Every time a peer responds positively, its participation value of *y* will increase by 1. $t_{hi} = \sum_k((CR)_{hk} + (nL)_{ki})$, $t_{hi} = \vec{T_k}$, $(CR)_{hk}'$ is a matrix and local trust value $(nL)_{ki}$ is the vector $(n\vec{L})$ such that $\vec{t_k} = (CR) + (n\vec{L})_k$. Global trust view produced by recursive view of transitive trust, $T^k = (CR) + (T^{k(i)})n$, where *k*(*i*) is the acquaintance of the peer *k*.

Suppose S_{ij} is the similarity between p_i and p_j trust values, about the same set of neighbors, and defined as the cosine angle between $\vec{Q}_i$ and $\vec{Q}_j$, then S_{ij} is calculated as follows: $S_{ij} = \frac{\sum_{x\in N_{ij}}(nL)_{ix}\times(nL)_{jx}}{\sqrt{\sum_{x\in N_{ij}}(nL)_{ix}^2\sum_{x\in N_{ij}}(nL)_{jx}^2}}$, if $\left\|\vec{Q}_i\right\|! = \left\|\vec{Q}_j\right\|! = 0$, and $S_{ij} = 0$, if $\left\|\vec{Q}_i\right\| = 1$, or $\left\|\vec{Q}_j\right\| = 0$. $[S_{ij}]$ denotes the matrix of common neighbor similarity trust as illustrated in fig. 3, and *n* denotes number of peers. Recommendations can be computed by: $(RS)_{ij} = \sum_k S_{ik}S_{kj}$. Peer p_i can get indirect similarity with the help of p_h and p_k whose similarity can be calculated directly. It is sensible to weigh p_j's similarity by the similarity of p_h and p_k while taking S_{ih} and S_{ik} as the trustworthiness of p_h's and p_k's feedback about p_j. Indirect similarity can be computed as follows: $(RS)_{ij} = S_{ih}\times S_{hj} + S_{ik}\times S_{kj}$. A group formed is viewed at higher level in terms of ability to detect malicious nodes.

D. Algorithm Design

The common neighbor similarity algorithm implicitly shows how to compute trust metrics. There is a strong relationship with the sizes of the trusted graphs, and the highest number of edge-disjoint paths. Edge disjoint paths problem is NP-Complete and is closely related to multi-commodity flow problem. A graph is called k-edge-connected if $\lambda \geq k$ and there exist at least k edge-disjoint paths between them. Similarly, it is called k-vertex-connected if $\lambda \geq k$ between every pair of unconnected vertices. If the paths are only required to be edge-disjoint, they can be constructed in polynomial time, using standard maximum flow algorithms. Given a trusted graph G = (V,E) and two peer nodes v and w, we find the trust value from v to w, and then the highest edge disjoint. The proposed neighbor similarity algorithm is shown below.

Algorithm 1: Common Neighbor Similarity Trust

```
Input: Graph $G$ = ($V$, $E$), $v$, $w \in V$ and Trust value $t(i, j)$,$\forall(i,j) \in E$
Output: Trust value $t(i, j)$
For $i$ = 1 to $n$
  For $j$ = 1 to $n$
    $\delta_i$ = (In-edgeSimilarity + Out-edgeSimilarity)
    $\delta_j$ = (In-edgeSimilarity + Out-edgeSimilarity)
    IF $\delta_i \geq \delta_j$ Then
      $t^{\bullet}(i, j) = t(i, j)\delta_i^{-1}$
    Else
      $t^{\bullet}(i, j) = t(i, j)\delta_j^{-1}$
    endIF
  end
end
```

E. Trust Relationships

An algorithm is used to build the relationship between Interest-based groups and peers. A peer accumulates no trust value at this time which ensures there is no peer interest bias similarity in choosing neighbor peers. If there are N nodes in the network, the definition of network average group coefficient is: $C = \frac{1}{N} \sum_{i=1 \cdots N} \frac{2p_i}{q_i(q_i-1)}$, where q_i denotes the number of neighbors of peer H_i, and p_i represents the number of logical connections between the q_i neighbors. A pair of neighbor peers may have direct or indirect relationship, where the edge values are a measure of how much p_A trusts p_B in e-commerce transactions. Let $max(x,\ y)$ be the maximum value of x and y. The direct relationship, $T(G_A, G_B)$ denotes how much group G_A trusts group $_B$. In a system with Q groups, trust is calculated: $T(p_i, p_k)$ = $R(G_A, G_B) \times \ln(\sum_{j=1}^{n} T(p_i, p_j) T(p_j, p_k)) n^{-1}$ + 1

VI. Performance Evaluations

Our network model consists of peers interacting and making business transactions. Freely evolving P2P networks have been shown to exhibit power-law network characteristics. Upon joining the network, peers connect to a peer i with probability: $\frac{d_i}{\sum_{j \in N} d_j}$, where N denotes the set of peers currently in the network, and d_i denotes the peer degree of peer i.

We create peer groups and assign peers at random to the groups based on peer's affinity towards a particular category of interest. In our work we vary the number of malicious peers that will exist in various groups.

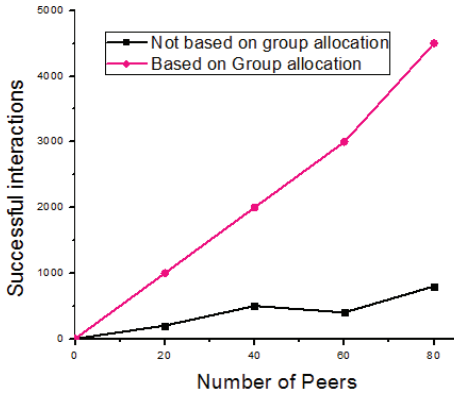

Fig. 3. Graph showing peers based on group allocation and not.

A. Effect of Grouping

In our set of experiments we show the effectiveness of grouping in a P2P e-commerce environment. If the number of peers that have similarity interest p is N, and of which M pairs are neighbors, we define the connection ratio of similarity interest p as, $IR(p) = \frac{M}{N}$. For specific peers set similarity interest p, the higher of $IR(p)$, the better its group effect. Managing a group in P2P e-commerce improves scalability of network. The groups help to weed out the malicious peers. We ran an experiment consisting of 100 peers involved in 100 simulation runs resulting to 1000 interactions as in table 1 above. Our P2P e-commerce community has a total of 40 different categories of interest. The transaction interaction is either successful or unsuccessful. We run three set of experiments: a) Group allocation and without group allocation as shown on Fig. 3; b) Transactions with 0% to 80% malicious peers as shown on Fig. 4, the graph show comparison of Eigen Group Trust and Neighbor Similarity Trust; c) Peers in groups compared with ordinary peers as shown in fig. 5.

B. Peers Based on Group Allocation

The Fig. 3 shows comparisons of peers based on with and without group allocation. It illustrates the message transmission among the peers. Peers discover groups depending on their interest. A group is updated as the peers attain membership, as trust is a dynamic evolutionary process. Cosine function is used to simulate the peers.

TABLE I
Peer Simulation Parameters

Network Parameters	Values
Number of Peers	100
Percentage of Malicious Peers	0% - 80%
Number of Interactions	< 5000
Maximum Number of categories of Interest	40
Number of Simulations runs	100

C. Improvement over Eigen Group Trust

Evaluation performance of proposed groups with neighbor similarity interest is compared to Eigen Group Trust model

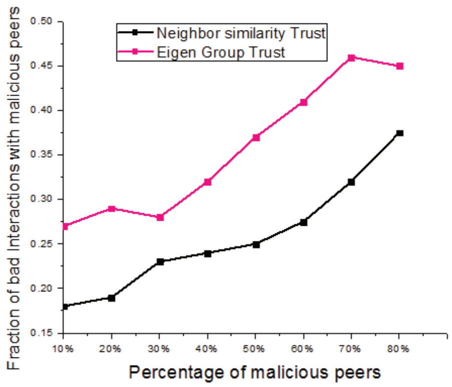

Fig. 4. Transactions between Peers in Group with malicious peers.

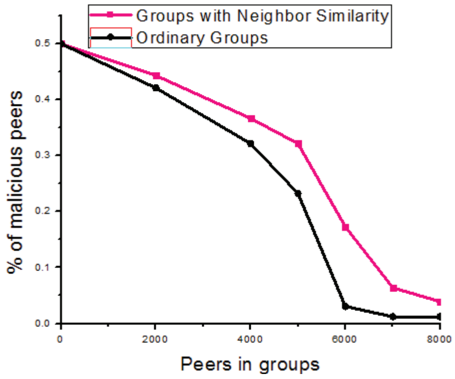

Fig. 5. Graph showing group with neighbor similarity and ordinary groups.

proposed by [4]. For a typical P2P e-commerce, peers can request for services and respond to requests. Malicious peers are more likely not to reward good services they receive. Fig. 4 accesses the effect of interaction with different percentage of malicious peers.

D. Neighbor Similarity and Ordinary Groups

The simulation is based on iteration. If a selected peer is malicious, it contributes a malicious service. The proposed method enhances reduction of maliciousness among the group members, by establishment of trust relationship between peers based on common interest. Groups help increase peer resource query hit rate, and decrease resource location time. Simulations on peers are run considering groups with neighbor similarity and ordinary groups. Fig. 5 shows the results of our simulation.

E. Security Analysis

In to ensure the security of the P2P e-commerce transactions, we employ key revocation and group key refreshing mechanisms. Anyone can join the “similarity net” to malicious interest, hence to address the threats caused by peers which leave and join the group:

- *Backward Secrecy*: new joined group members must have no access to past group communication.
- *Forward Secrecy*: revoked group members must have no access to future group communication.

We can also safeguard the group by ensuring that data is encrypted.

VII. Conclusion

Trust has been studied for many years, particularly in P2P networks, social networks, and mobile ad-hoc networks. Trust in P2P e-commerce is relatively new. Our proposed group formation offers a solution to reduce malicious peers. This creates confidence among business partners. It employs similarity interest trust based on neighbors to maintain trustworthiness. The method reduces malicious behaviors i by comparing relatively the limited number, and fluctuation rates of peer’s interests. The issue of undiscovered group has not yet been addressed. More on common neighbor similarity should be investigated by use of social communities to achieve the benefits of decentralized P2P e-commerce.

Acknowledgments

This work is supported by National Natural Science Foundation of China under grant numbers 61073037 and 61103035, and Hunan Provincial Science and Technology Program under grant numbers 2010GK2003 and 2010GK3005.

References

[1] Y. Zhang, H. Zheng, Y. Liu, K. Li, and W. Qu, GroupTrust model based on service similarity evaluation in P2P networks, *journal of intelligent systems(2011)*, DOI 10.1002/int.20452, pages 47-62.

[2] L. Mekouar, Y. Iraqi, and R. Boutaba, An analysis of peer similarity for recommendations in P2P systems, *Journal of Springer Science and Business Media (2010), Multimedia Tools Applications, DOI 10.1007/s11042-010-0612-1*, pages 1-27.

[3] A. Ravichandran and J. Yoon,Trust management with delegation in grouped peer-to-peer communities, *SACMAT (2006)*, pages 71-80.

[4] S. D. Kamvar, M. T. Schlosser, and H. GarciaMolina, The EigenTrust algorithm for reputation management in P2P networks, *in:Proc. of ACM WWW (2003)*, pages 640-651.

[5] J. S. Xu and L. J. Zhong, A Reputation-based trust mechanism for P2P e-commerce Systems, *journal of software (2007)*,Volume 10, pages 2551-2563.

[6] L. Tang, Grouping based mechanism driven by reputation in P2P e-commerce, *Academy publisher, WISA (2009)*, pages 510-515.

[7] L. Sun, L. Jiao, Y. Wang, S. Cheng, and W. Wang, An adaptive group-based reputation system in P2P networks, *WINE, LNCS (2005)*, pages 651-659.

[8] C.W Hang, Y. Wang, M.P Singh, Operators for propagating trust and their evaluation in social networks. *in:Proc. AAMAS, SC, IFAAMAS (2009)*, pages 1025-1032.

[9] I. Keidar, J. Sussman, K. Marzullo, and D. Dolev, A group membership service for WANs, *in:Proc. ICDCS, ACM Press (2000)*, pages 356-365.

[10] W. Ji, S. Yang, D. Wei, and W. Lu, GARM: A group - anonymity reputation model in peer-to-Peer system, *IEEE (2007)*, pages 1-8.

[11] B. Bultena, B. Grunbaum, and F. Ruskey, Convex drawings of intersecting families of simple closed curves. *in:Proc. CCCG (1999)*, pages 18-21.

[12] L. Chen and J. Liang, The research of trust model based on group-recommend in P2P network, *IEEE(2008)*, pages 845-848.

[13] D. Liben-Nowell and J. Kleinberg, The link prediction problem for social networks, *in: Proc. CIKM, ACM Press(2003)*, pages 1-4.

[14] N. Liu, J. Li, L. Hao, Y. Wu, and P. Yi, Group-based trust model in P2P system based on trusted computing, *in:Proc. CSSE, IEEE (2008)*, pages 797-801.