Inferring Trust In Web-Based Social Network Using Social Impact Theory

Arambam Neelima, CSE Department, National Institute of Technology Manipur

Heisnam Rohen Singh CSE Department Assam down town University

Lourembam Suraj Singh, CSE Department Mizoram University

Sarangthem IbotombiSingh CSE Department Tezpur University

Abstract

Web based Social networks allows people to find and know other people that share same interest. As web based social networks are virtual social place, the relationships in web based social networks are more complex and the information provided by the user may not be trustworthy to all. A mechanism is needed to infer trust from one person to another that is not directly a friend of the user and there should also be a feature for users to specify how much they trust their friend. Our paper looks particularly at inferring trust from friends about their friends.We gave an introduction to the concept of trust in web based social network and its properties, then present a model for inferring trust between individuals that are not connected in the network based on Andrzej Nowak's social impact theory. The trust value for an individual will be a continuous value ranging from 0 to1. This model considers the effect of social distance between the individuals and the impact of its environment while inferring the trust. As trust is personal and people's needs are different in different situation, we introduce a user input variable δ that will categorize the trust value as trustworthy or untrustworthy. Each individual can have different δ value. We consider only the current state of the social networks without considering the history or any learning approaches.

Keywords: *Social network, social distance, social impact theory, trust*

1. Introduction

In recent years, there has been a rapid increase in web based social networking sites popularity. A social network is a social structure made up of individuals called "nodes" where the individuals that share same interests and/or activities are connected. The relationships in web based social network are more complex than a simple indication that two people know one another. The web based social network is just a virtual social place, the information provided by the user may not be trustworthy to all. In social network, users assign a trust rating describing their connections to others. Some social networks even have trust implied inside their network connections. As the increase in popularity of social networking is on a constant rise, there is a need for inferring trust relationships between individuals that are not directly connected.

1.1 `Meaning and properties of Trust.

Trust plays an important role across many disciplines and each discipline has defined the trust in different ways. Trust is usually specified in terms of a relationship between a trustor, the subject that trusts a target entity, and a trustee (i.e., the entity that is trusted). In the following we review the various definitions and suggest a definition applicable to Internet services

The European Commission Joint Research Centre defines trust as "*the property of a business relationship, such that reliance can be placed on the business partners and the business transactions developed with them"*

The Oxford Reference Dictionary states that trust is "*the firm belief in the reliability or truth or strength of an entity*."

Sztompka[8] states that "Trust *is a bet about the future contingent actions of others*". There are two main components of this definition: belief and commitment.

Tyrone Grandison and Morris Sloman, define trust as "*the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context*" (assuming dependability covers reliability and timeliness). They also define distrusts as "*the lack of firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context."*

We define trust as a belief, surety or a confident expectation that the trustee will perform an action important to the trustor that will lead to a good outcome. There are four main properties of trust, namely transitivity, asymmetry, personalization and composability[3].

1.1.1 Transitivity

Trust is not perfectly transitive but it supports the idea of transitivity. Transitivity describes how trust can be passed back through a chain of people. If person A highly trust person B and B highly trust C, it doesn't always and exactly follow that A will highly trust C. However, as stated earlier trust is a belief that the trusted person will perform actions that will lead to a good outcome. If A asked B whether or not C is trustworthy, A will take B's opinion on C because A believes that B will give her information that will lead to a good outcome.

1.1.2 Asymmetry

Trust is asymmetric in nature. A trust relationship can be one-to-one between two entities, however it may not be symmetric. It is not identical in both directions as each individual has different perception, experiences, thinking or opinion. If A trust B ,it is not necessary that B should also trust A.

1.1.3 Personalization

Trust is a personal opinion. Individuals have different perception or opinion about the same thing. So trust is based on the perspective of the user. There is no correct or incorrect trust value except when considered from the perspective of a given individual.

1.1.4 Composability

Trust can be composed into a single value. Composability of trust is important feature for making trust computations. Trust information from many sources needs to be composed into a composition function that can vary from situation to situation and person to person.

2. SOCIAL IMPACT THEORY

Social impact theory[4] is a model that conceives of influence from other people as being the result of social forces (pressures from other people) acting on individuals. The social impact theory describes how individuals feel the presence of their peers and how they in turn influence other individuals. The social impact on a subject depends on the size of the groups, on their convincing power, and on the distance from the subject. Starting with a population of N individuals, Each individual 'i' is characterized by an opinion $\sigma_i = \pm 1$ and by two real-valued parameters that estimates the strength of its action on the others: *persuasiveness* p_i refers to the ability to convince someone with an opposing position to change, and *supportiveness* s_i refers to the ability to help those who agree with someone's own point of view to resist influence from others. The total impact I_i that an individual i experiences from his or her social environment is

$$I_i = \left[\sum_{j=1}^{N} \frac{p_j}{d_{ij}^{\alpha}} (1 - \sigma_i \sigma_j)\right] - \left[\sum_{j=1}^{N} \frac{s_j}{d_{ij}^{\alpha}} (1 + \sigma_i \sigma_j)\right] \quad (1)$$

where $\alpha > 2$ expresses how fast the impact decreases with the distance d_{ij} between two individuals. The first term gives the pressure exerted by the individuals with opposite opinions and the second term gives the pressure exerted by the individuals with the same opinion. So, whenever the impact on an individual from a group with a different opinion is greater than the impact of his or her own group, the attitude of that individual changed.

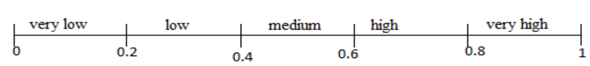
The new opinion at time t+1 will be expressed by the given rule

$$\sigma_i(t+1) = -sgn[\sigma_i(t) + h_i],$$

Where h_i is a random field representing all sources other than social impact that may affect the opinion.

3. Proposed Model

The social network will be modeled with a directed graph G=(V,E). Each individual in the network will be represented by the vertices of the graph. The edges in the generated graphs represent connections (friendship or acquaintances) between individuals and the edges are augmented with trust values (continuous value) representing the trust between individuals. Each individual will have a trust rating for their neighbors or their friends (connected individuals). The trust value will range from 0 to 1.



However, the trustworthiness of an individual is governed by a user input parameter, δ called minimum expected trust value. As trust is personal and people's needs are different in different situation or different scenarios, One can consider person with 0.6 trust value as a trustworthy person for simple purposes but it is not good enough to consider trustworthy regarding a financial transactions, some people may even consider 0.5 trust value as trustworthy. So, trustworthiness of an individual will be determined by the input parameter δ. Individuals with trust value greater than or equal to δ will be considered as a trustworthy otherwise an untrustworthy person.

The source will poll from a set of nodes (vertices),say M. Set M will be comprised of all the neighboring nodes of the source node that has a direct link with the sink node.

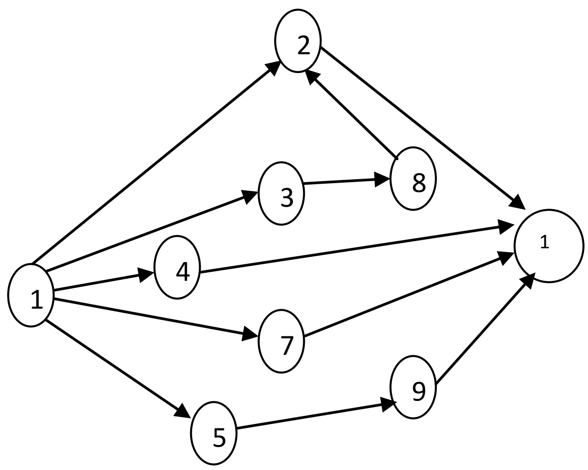


Fig.1:Graphical representation of a social network

Figure.1 depicts a sample social network. Let node 1 be the source node and node 10 be the sink node, then the set M will consists of {2,4,7}

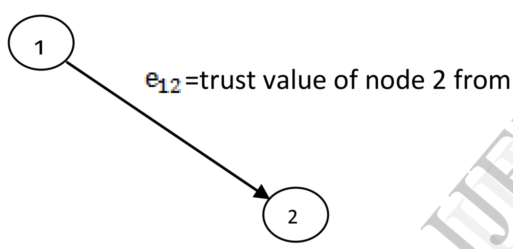


Fig2: Edge representing the trust value.

Each node in the set M will calculate the impact experienced from the social environment using the following expression

$$I_i = \left[\sum_{j=1}^{N} \frac{p_j}{d_{ij}} (1-\sigma_i^{'}\sigma_j^{'})\right] - \left[\sum_{j=1}^{N} \frac{s_j}{d_{ij}} (1+\sigma_i^{'}\sigma_j^{'})\right]$$

where, N is the set of neighboring nodes of node i in set M

$N = \{V\}\ ,\forall\ V_j \in M \text{ and } e_{ij} \text{ exists}$.

p_j = persuasiveness of the node j.

s_j = supportiveness of node j

d_{ij} = distance between the two nodes i and j.

σ_i = node i's opinion about the sink node.

The first term of Eq.(1) gives the pressure exerted by the individuals that are against the node i's opinion of sink node and the second term gives the supportive impact i.e. the pressure exerted by the individuals with the same opinion as node i's opinion on the sink node. If the first term is greater than the second term (i.e. I_i is a positive value) then the node i will be forced to flip its opinion regarding the sink node and if the second term is larger than the first term, then the node I will retain its opinion. If I_i is a positive value, then node i will flip its opinion. The new opinion will be the average trust values of those individuals that were against the node i's opinion.

Mathematically,

$$\sigma_i(t+1) = \frac{\sum_{j=1}^{z}\sigma_j}{z} \qquad (2)$$

where Z is the subset of N comprising of individuals that has different opinion with I regarding the sink node.

The following cases can be observed after the calculation of the Impact (I) using Eq. 1

Case 1: When the impact of the node's environment is negative i.e. they support the node's opinion about the sink node

a) Trustworthy

If node i's trust rating regarding the sink node is trustworthy, then the node will retain its opinion or trust rating about the sink node.

b) Untrustworthy

If node i's trust rating regarding the sink node is untrustworthy, then the node will retain its opinion or trust rating about the sink node.

Case 2: When the impact of the node's environment is positive i.e they are against the node's opinion about the sink node.

a) Trustworthy

If node i's trust rating regarding the sink node is trustworthy, then the node will flip its opinion or trust rating about the sink node using Eq.2.

b) Untrustworthy

If node i's trust rating regarding the sink node is untrustworthy, then the node will change its opinion or trust rating about the sink node using Eq.2

Sl no.	**Node's trust rating**	**Impact**	**Result**
1.	trustworthy	-ve	trustworthy
2.	untrustworthy	-ve	untrustworthy
3.	trustworthy	+ve	untrustworthy
4.	untrustworthy	+ve	trustworthy

3.1 Calculation of indirect trust

In the beginning, there will be frequent changes of opinion as each individual lost and gained its stand. These steps continued until there were no further changes in opinions in successive runs. Finally**,** each recommender will be returning a trust value (t) regarding the sink node (trustee). But there will be two clusters with different opinion and the source node will determine how much he/she can trust the sink node depending on the percentage of the highly rated node (rating>0.5) present in each cluster. Three different cases may arise.

Case I: Either or both the cluster contains highly rated node. If any of the two clusters consists of highly rated node, then the source will calculate the indirect trust using the following steps.

a. If $\left(\frac{\text{total no.of highly rated nodes in cluster1}}{\text{total no of nodes in cluster1}} > \frac{\text{total no.of highly rated nodes in cluster2}}{\text{total no of nodes in cluster2}}\right)$

b. Indirect trust=average trust value of cluster1;

c. Else

If $\left(\frac{\text{total no.of highly rated nodes in cluster1}}{\text{total no of nodes in cluster1}} < \frac{\text{total no.of highly rated nodes in cluster2}}{\text{total no of nodes in cluster2}}\right)$

d. Indirect trust=average trust value of cluster2

e. Else, Indirect trust=average trust value of the cluster which has larger no of highly rated node;

Case II: If there is no highly rated node in both the clusters i.e. all the nodes in the cluster provides irrelevant information, then the indirect trust will be calculated as the difference between the maximum trust value and the average trust value provided by the larger cluster.

Indirect trust=1-average trust value of the larger cluster.

Case III: It might happen that all the nodes are newly joined and haven't participated in any recommendation i.e. unrated nodes. In that case the average trust value of the larger cluster will give the indirect trust.

4. Implementation Details.

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 fonts are preferred.

We implement the above proposed model using an agent based modeling and simulation system called Repast Symphony. Agents will have a dynamic relationship with other agents. Agents will be having their own trust value, persuasiveness, supportiveness and rating as their characteristics. We start our implementation with the creation of a random graph representing our social network. We have implemented our model with two different datasets.

a) Random Data
b) Advogato Dataset

5.1 Experimental set up for implementation using random data

5.1.1 Creation of the random graph

A random graph is obtained by starting with a set of *n* vertices and adding edges between them at random. We will be creating our random graph based on Erdős–Rényi model for generating random graph. The output of Erdős–Rényi model is a directed graph with self loop so we made a little change in the original algorithm to make it a directed graph without self loop(as required). Before generating a uniform random number in step 4 we make sure that the indexes (i.e. i and j) of the vertices are not the same.

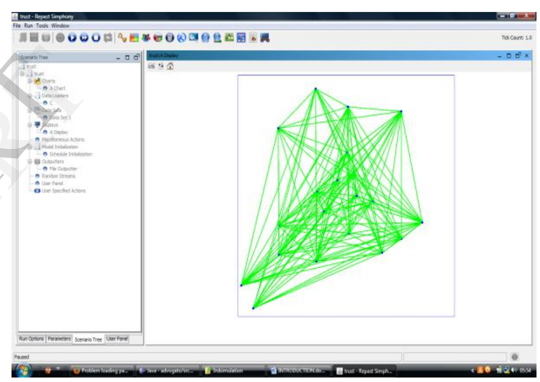


Fig 3: Snapshots of a random graph based on Erdős–Rényi model

5.1.2 Simulation

We simulate our model in two different types.

a) Simulation under different behavior of the recommender

At first tick we run our model with a random trust value of the trustee. After every interval of 1 ticks we randomly change the type of the recommender and also changing the trust value of trustee. We run it in different situations like making most of the recommenders honest or dishonest or giving a mixture of honest and dishonest recommenders

b) Simulation under different network structure

At first tick we run our model with a random trust value of the trustee. After an interval of 1 ticks we randomly change the structure of the network keeping the trust value of trustee in constant. We change the structure of the network by randomly adding or removing few links between the recommenders or even adding some new recommenders.

5.2 Experimental set up for implementation using Advogato datasets

5.2.1 Creation of the graph

Each account on Advogato corresponds to a node in the graph. An edge exists from node *s* to node *t* when account *s* has certified account *t* at level *l* or higher. We generate the graph by starting with a set of 200 vertices representing the 200 accounts(users) and adding edges between them as found in the Advogato dataset. Each edge has a level giving the relationship quality between the users.

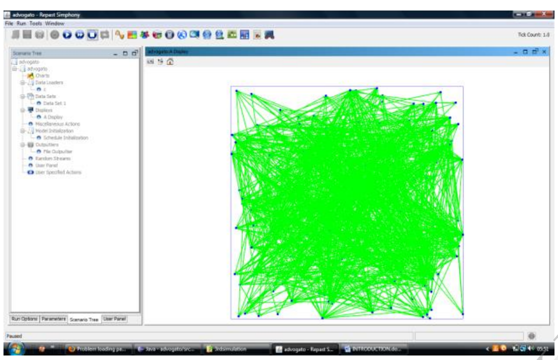


Fig.4: Snapshots of the graph generated , based on Advogato datasets.

5.2.2 Simulation

At first tick we run our model with a random trust value of the trustee. After an interval of 1 tick we randomly change the trust value of the trustee.

6. Result

6.1 Results obtained from data that are generated randomly

Different behaviors of the recommenders

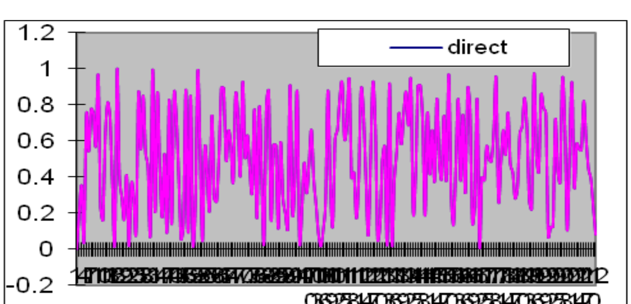


Fig.5: Direct trust Vs. Indirect trust when all the recommenders (100%) are honest

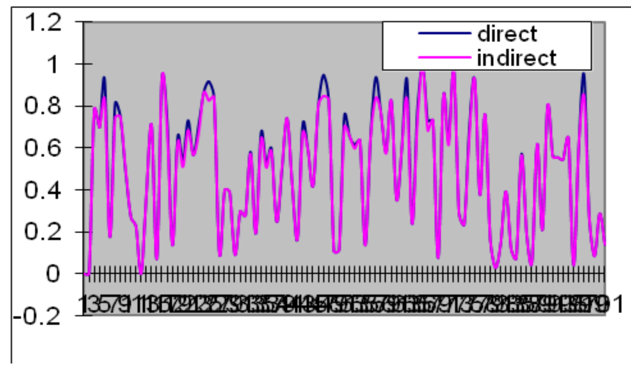


Fig.6: Direct trust Vs. Indirect trust with 50% recommender of honest type, 25% recommender of mix type and remaining 25% recommender of dishonest type.

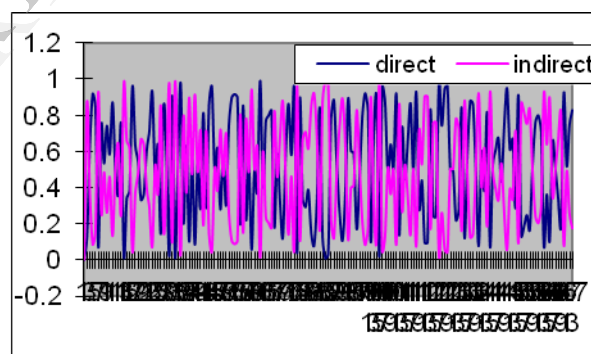


Fig.7: Direct trust Vs. Indirect trust when 75% recommenders are dishonest and 25% recommenders are honest

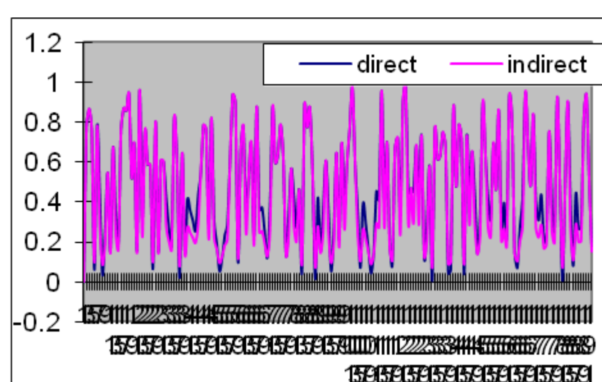


Fig.8 Direct trust Vs. Indirect trust with 50% recommenders of honest type and 50% recommenders of mix type

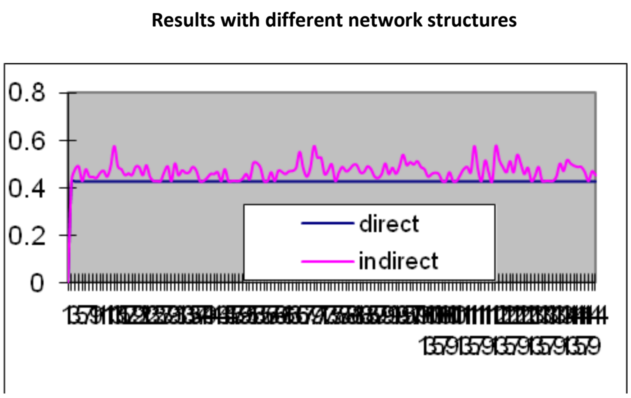


Fig.9 Direct trust Vs. Indirect trust with different network structure.

6.2 Results obtained from Advogato datasets

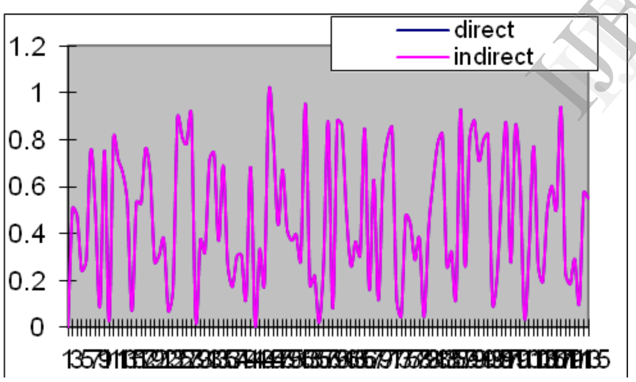


Fig10 Direct trust Vs. Indirect trust.

7. Conclusion.

The different simulation shows that, the indirect trust is almost similar with the direct trust. From fig.5,6,7,8,9,10 we can infer that the generated indirect trust depends on the type of the recommender. Adding a rating mechanism to denote the quality of the relationship between the users can help us in classifying the dishonest, honest and mix type of recommender. The trust model makes use of the quality of relationship between the users.

8.References

[1] Audun Jøsang.Trust-Based Decision Making For Electronic Transactions. In Proceeding of the Fourth Nordic Workshop on Secure Computer Systems (NORDSEC'99), 1999

[2] Agent based model< http://en.wikipedia.org/wiki/Agent-based_model>

[3] Jennifer Ann Golbeck and James Handler "*computing and applying trust in web based social network*", 2005. < http://trust.mindswap.org/papers/GolbeckDissertation.pdf>

[4] Masoud Akhoondi, Jafar Habibi, Mohsen Sayyadi, *"Towards a Model for Inferring Trust in Heterogeneous Social Networks"*, 2008 Second Asia International Conference on Modelling & Simulation, 2008*",* pp.52-58.

[5] Mohsen Lesani and Saeed Bhageri,."*Applying and inferring fuzzy trust in semantic web social network*" < http://www.springerlink.com/content/w44536p631916023/fulltextpdf> 2006

[6] Nowak, A., Szamrej, J., & Latane, B. From private attitude to public opinion: A dynamic *theory of social impact.* Psychological Review, 97, 362-376.,1990,

[7] Nobari et al, "Fast random graph generation", *Proceedings of the 14th International Conference on Extending Database Technology* (Uppsala, Sweden: ACM),2011.

[8] Sztompka P. "*Trust A sociological theory*", Cambridge university Press,Cambridge UK, 1999.

[9] Social network, Wikipedia <http://en.wikipedia.org/wiki/Social_network>.

[10] Agent based model< http://en.wikipedia.org/wiki/ Agent -based_model>