Social Network Collaborative Filtering Framework and Online Trust Factors: a Case Study on Facebook

Wei Chen, Simon Fong
Department of Computer and Information Science
University of Macau, Macau SAR
ccfong@umac.mo

Abstract

Recommender systems have been proposed to exploit the potential of social network by filtering the information and offer recommendations to a user that he is predicted to like. Collaborative Filtering (CF) is believed to be a suitable underlying technique for recommender systems on social network, because CF gathers tastes of similar users; and social network provides such a collaborative social environment. One inherent challenge however for running CF on social network is quantitative estimation of trust between friends. Although many researchers investigated trust metrics and models in social network, none so far has efficiently integrated them in a CF algorithm. The contribution of this paper is a framework of collaborative filtering on social network, and a novel approach in measuring trust factors by data-mining over a survey dataset provided by The Facebook Project.[1] The quantitatively estimated trust factors can be used as input parameters in the CF algorithm. Facebook is taken as a case study here to illustrate the concepts.

1. Introduction

Social network has grown in tremendous popularity in recent years as a social platform on which friends share information and interact via cross-postings, messaging, games, social events and applications. The potentials of such a distributed and highly connected social online platform have been exploited recently for user-centric applications.

Recommender system is one of such applications that offer recommendations to a user by gathering similar users and filtering their information over a social network. Commonly there are two types of filtering techniques used in recommender systems, item-based and collaborative-based. Item-based filtering looks at the attributes of items that a user purchased or favored before, and it attempts to find other items that have similar attributes and recommend them to the user. Collaborative filtering (CF) on the other hand focuses on user data, and makes automatic predictions about the interests of a user by collecting taste information from many users who share a similar background and preferences. CF naturally would fit well in social network environment since a large collaborative web of user data is readily available in contrast of a website which is usually represented by a static repository of product information.

Although CF is believed to work well in social network environment, measuring trust is a challenging task due to the decentralized and virtual nature of social network. For instance a recommendation made by a family member would be perceived more trust-worthy than that by an added online 'friend' from a social network which you may have never met before physically.

In Facebook, for example, a pair of users who have added each other as friends could be briefly categorized as family, friends, and friends-of-friends. There are other relations such as colleagues, members of a same group and activities jointly mingled – they reflect quite a good mix of explicit and implicit relationships on a social network.

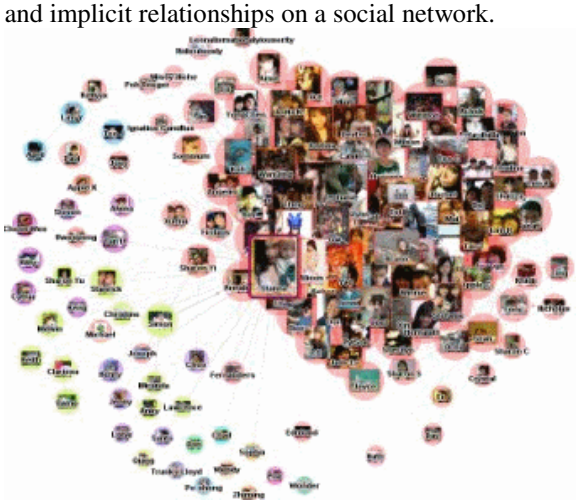

Figure 1. Visualization of friends on Facebook by strengths of relations

[1] http://www.thefacebookproject.com

2. Research Motivation

Figure 1 is illustrated as an example of clustering friends on Facebook by the strengths of relations via a visualization program. You can see an obvious clan is formed where friends who are explicitly related (such as family and colleagues) and implicitly related via collaborative activities and postings were drawn near.

How to measure the trust factors, the strength, and the magnitude? How to model these factors quantitatively and more importantly integrate them into a CF algorithm? These are the prominent questions to be answered before a recommender system powered by CF can be effectively deployed on a social network.

Trust metrics have been studied extensively by many researchers in the past. Likewise CF stems from the earlier system of information filtering, is a mature technology that has been widely researched and adopted in many online scenarios. There however exists a gap between the two areas, especially on social network like Facebook where the concept of trust is fuzzily defined.

The objective of this research is to bridge the gap by proposing a collaborative filtering framework that is specifically designed to operate in a social network environment. In particular, the similarity measure between profiles of a pair of users and the trust between them are fused into the CF algorithm. (For simplicity, trust between two users is assumed symmetrical.) Data of user profiles are either readily available or technically be obtained using API from Facebook and other social networks. Online trust factors would be formulated through analysis and inferring from given live datasets. As a novel approach, we applied data-mining algorithms (decision tree and association rules) to derive the relative importance of factors in social activities that contribute to overall trust. The results in turn are adopted by the CF algorithm for achieving information filtering based on users' similarity and the trust between them.

The paper is organized as follow: Section 3 reviews related works on CF and trust metrics. Section 4 is our proposed framework of Social Network Collaborative Filtering. Section 5 models about trust factors by using a latest user survey dataset pertaining to Facebook. Prediction trees are built based on the data, as well as association rules are obtained that shed some insights about the impacts of each factors of social attributes on the overall trust measure. Inferring from the cumulative gains of Lift Charts in the process of building decision trees, the relative importance between the factors are estimated. A conclusion is drawn at the end in section 6.

3. Related Works

Massa extended traditional recommender systems to Trust-aware recommender systems [1] by inputting a trust matrix (representing all the community trust statements) in addition to the ratings matrix (representing all the ratings given by users to items). The trust matrix is based on the concept of 'web of trust' which is formed by letting the users to explicitly rate about the trust on the other users. The design is based on epinion.com and PageRank [2] which are not exactly social platforms. In contrast, our CF framework considers the activity information on Facebook and from there estimates the trust level between a pair of users without needing them to explicitly express or rate about the trust on each other. As pointed out by Massa, the topic of trust metrics [3, 4, 5] is very recent and there aren't thorough analysis of which metrics perform better in different scenarios. Our method sheds light on formulating a trust model that is characterized by features of Facebook. Massa's architecture is elegant as the trust matrix can be replaced by more sophisticated ones. There is a future opportunity of coding a trust matrix derived from Facebook data and integrated into Massa's architecture.

Other variants of Massa's trust-aware recommender systems emerged in recent years, such as Reputation-based Trust-Aware Recommender System [6] that includes the social factors e.g. user's past behaviors and reputation together as an element of trust; another one called trust-aware recommender model (TARM) [7], which can utilize trustworthy experts and their search experiences to recommend their search histories to the common user according to profile similarity between common user and experts; and last year the same authors extended the model [8] by replacing the similarity weight with trust weight by trust propagation over the trust network, and they proposed that trust decreases along propagation.

Specifically targeted for online social network, Kazienko [9] proposed a general recommendation framework. It integrates many sources of data in order to generate the relevant personalized recommendations for social network members. The sources include relationships between people, and users' profiles. The relationships between people are represented by a social statement of the user in the network that consists of two data sets: general, aggregated openness and activities features of this user in relation to all others, also in the past, and measures of the relationship between this user and other members of the network. The user profile contains components of activity that measures the activity of the user within the community, and relationship that describes the number and duration

of the users' relationships and some other features that characterize them. The framework is almost perfect in consideration of most if not all social elements, except the weight (or significance) scales of those social elements that contribute to an extent of trust between two users. This paper is focused on integrating the measures of trust on the relationship between social network users, and estimating the scales of those elements, for improving Kazienko's recommendation framework.

4. Proposed Framework

We proposed a social network recommender framework based on CF that extends from [9] by including the dimension of trust, namely Collaborative Filtering Trust Network (CFTN). Similar to the framework [9], CFTN gathers many sources of data both static and dynamic for generating a recommendation.

The static attributes are obtained from users upon signing up an account on social network. The ever happening activities are represented by the dynamic attributed that are monitored and gathered by the system.

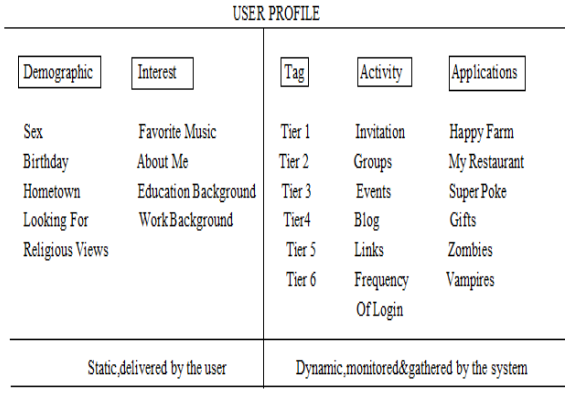

Figure 2. User's profile

In addition to these data stored in the profile a new indicator called tag is used to denote the level of trust perceived by the user to a corresponding friend in his/her friends list. In this example, arbitrarily we chose 6 tiers to signify the levels of trust by the relations that the user has towards her friend. On Facebook, a similar category of friends in the privacy are referred as friends, friends-of-friends and everyone. Combining with other relations such as family, colleagues, ex-classmates, etc, that can be easily mapped to the six tiers as selected by the user.

In our CFTN framework, we monitor activities in order to calculate similarity, while tags are used to compute the trust value.

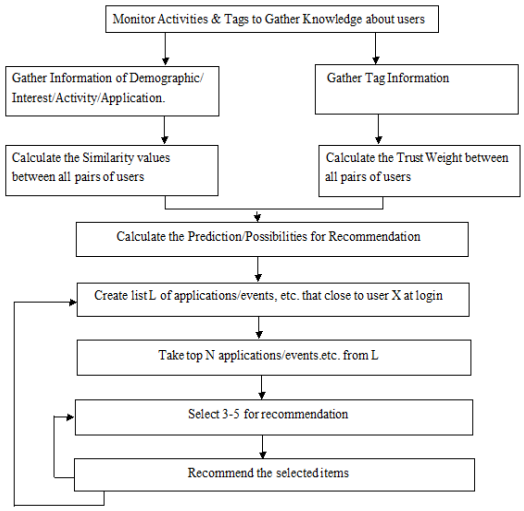

Figure 3. CFTN Framework

The workflow of the framework is shown in Figure 3. For details of the basic mechanisms readers are referred to [9] and [1] since this model is based on its predecessors. We highlight however the similarity measures by the CF algorithm and how trust is embedded in the calculation.

4.1. Similarity

Based on [10], the similarity between user u_i and u_j is aggregated by a series of difference functions $f(A_{ni}, A_{nj})$ with respect to each attribute in the user profile, between users i and j.

$$S(u_i,u_j) = w_1 f(A_{1i},A_{1j}) + w_2 f(A_{2i},A_{2j}) + \ldots + w_n f(A_{ni},A_{nj})$$

and $\sum_{n=1}^{n} w_n = 1$ where w_n is relative weights set in the system given to the difference in value of attribute An between users u_i and u_j. For example, we have two users who have the following attributes of interest as a part of the User Profile data. Assume that we have predefined the weights with respect to the interest attributes in the system as follow.

Table 1. Example attributes and weights

User / Attributes	u_i	u_j
Sex	Female	Male
Interested In	no	Diving
Interested In	Shopping	no
Interested In	Classic Music	Music

w_1	w_2	w_3	w_4
0.23	0.25	0.18	0.34

By the example, we could compute the similarity:

$S = 0.23\times0 + 0.25\times0 + 0.18\times0 + 0.34\times1 = 0.34$

The function f returns a binary value, f=0 or 1. Alternatively we could define $f \in (0,1)$ as a multiple value for handling ordinal data by Pearson function.

4.2. Trust by Relation

Though it might be debatable that whether trust can inferred in virtual environment, Gürsel and San [11] argued that people do it in real life and inferring trust for unknown people, i.e., people with whom a user has no direct connection, is a key research topic in trust-aware recommender systems. In [11], a referral system was developed based on an underlying concept of trust network.

A trust network (aka Web-of-Trust by [1]) infers trust between two people by the degree of connectedness [12] that carries a linear decay in propagating trust. That is, the shorter a distance it is away from the source node, the closer the friendship hence the trust it is to the user and vice-versa.

Applying the principle of trust network to our recommender framework, a variable JUMP count is used to symbolize the relationship between two users. The following figure shows an example snapshot of a model of trust by relation.

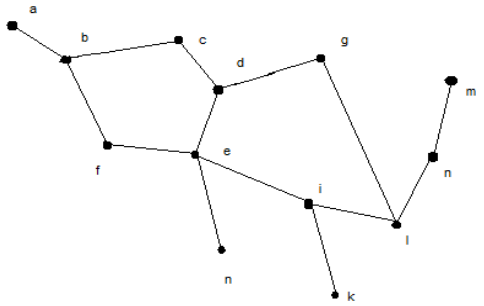

Figure 4. Trust by Relation Model

A suggested mapping of JUMP counts that correspond to the category of relations and tagging tiers is shown in Table 2.

Table 2. A example mapping of JUMP counts and tagging tiers

From Node *i* to *j*, JUMP times are/is	Tiers	Relationships
1	1	Family members (parents,children,close relatives)
2	2	Colleagues,non-close relatives
3	3	Ex-schoolmates(used to have the same taste)
4	4	Friends
5	5	Friends' friends
6 and up	6	Public

When users add new friends into their social network, they are asked to specify some types of relationship which could map to one of the tiers from 1 to 6. Different weights hence can be set to differentiate levels of trust $T_1 \sim T_6$, based on the significances of the attributes.

$$T_{i,j} = \prod_{i}^{j} T_{i,a,b,..m,j} = T_{i,a} \times T_{a,b} \times ... \times T_{m,j}$$

$$= T_1 \times T_2 \times ... \times T_5 \times T_6^{n-5}$$

where from nodes *i* to *j*, JUMP count = *n* times

For there could be multiple ways to reach one node from another node, the $\min\{T_{ij}\}$ is chosen as an optimistic choice which takes the least jump times according to a graph walking algorithm [13].

4.3. Trust by Reputation

Besides inferring from direct relations as in the case of connectedness in previous section, trust in social context may be derived from the reputation of a user which can be reflected from her social profile and the legacy she left behind.

Sociological definitions of trust generally have two major components as advocated in [14]: a belief and a willingness to take some actions based on that belief. In a virtual community, trust translates to belief that an information producer will create legitimate information, plus a willingness to commit some time to reading and processing it. Therefore if users can identify the information producers they trust online, then they will accept the information and work with them.

On a social network, the concept of circles of friends goes indeed beyond the friends who are related by bloodlines, by association or by referrals (as in the previous section). Quite often strangers who have never met mingle and develop trust online, which is exactly one of the unique features of social network. Usually the online users perceive each other by their reputations such as how well known they are among their peers in some specialized groups – who they are, and the traces of activities they left behind in the social community – what they do/did.

In general we call this kind of trust as Trust by Reputation. The reputation of a user can be cultivated by his profile, the contents and the activity history produced by the user. The information usually would be recorded on a social network site, over his pages and his acquaintances' pages; they can be observed over for evaluating how much he can be socially trusted.

The idea of quantifying trust metrics on social networks has been attempted by researchers [15, 16, 17]. For instance, Dwyer et al [15] applied statistical methods such as ANOVA analysis and correlation analysis to measure the levels of trust and privacy in a comparison of Facebook and MySpace. Dependent variables such as information shared in users' profiles and social communications are evaluated.

In our framework, we assume six attributes that can be observed from users' accounts on Facebook as elements that contribute to a user's reputation which in turn is a key factor to online social trust.

Table 3. Trust by Reputation attributes

Attributes	Metric
Personal Information	Completeness
Wall-to-wall Posts	Quality and Quantity
Inbox Messages Exchanged Frequency	Number
Number of Friends	Number
Number of Mutual Friends	Number
Groups in Common	Number

The trust value by reputation between user i and user j is then evaluated as follow, according to a simple Multiple Attribute Utility Theory (MAUT):

$$T_{i,j} = \alpha \frac{\sum PI}{totpi} + \beta \frac{\sum WTWP}{totwtwp} + \chi \frac{\sum IMEF}{totef} + \delta \frac{\sum NF}{totnf}$$

$$+ \varepsilon \frac{\sum NMF}{totnmf} + \phi \frac{\sum_{i=1}^{i=n} GIC_n}{totgic}$$

and $\alpha + \beta + \chi + \delta + \varepsilon + \phi = 1$, where, PI means personal information, $WTWP$ means wall-to-wall posts, $IMEF$ means the amount and frequency of inbox messages exchanged, NF means the number of friends, NMF means the number of mutual friends between user i and j, GIC means the number of groups in common, and Tot is prefix of total which is the total quantity of a particular attribute of a user.

The strength of the relationship $sr(i, j)$ is the measure that indicates how firm/strong the relationships between user i and user j in the social network. In this case, it is defined as: $sr(i, j) = w_s S(i, j) + w_t T_{i,j}$ where w_s+w_t=1, and T_{ij} could be chosen from the computation of Trust-by-Relation or Trust-by-Reputation. The weights w_s and w_t are used to control the importance between similarity and trust between the two users. The equation is supposed to be flexible that one can add or minus other factors whenever deemed fit.

In the past, CF algorithm allowed users to arbitrarily define the weight parameters. In our framework, we proposed that the weights assume the values from the trust factors which are estimated from a Facebook survey dataset. The following section shows how the values for the trust factors can be estimated.

5. Measuring Trust Factors

The remaining challenge now is to choose the factors and quantify the relative weights for the factors that would be embedded in the calculation of trust measure T. As there is yet a definite or standardized selection scheme of trust factors for considerations, some de-facto approach emerged as commonly agreed by most researchers. For instance Przemyslaw and Katarzyna [9] nominated the following for calculating the strength of a relationship: the number of emails exchanged, the number of the mutual readings and comments on their blogs, the number of common chats in specified time, etc. Some of these are included in our case as shown in Table 3.

It is pointed out that this range of elements can vary between systems and tightly depends on the functionality that the specific system provides. A recent study by Gilbert and Karahalios [16] generalized the trust factors in to seven tie strength dimensions and they have statistically shown how strong they and their predictive variables do relate to the trust in social network.

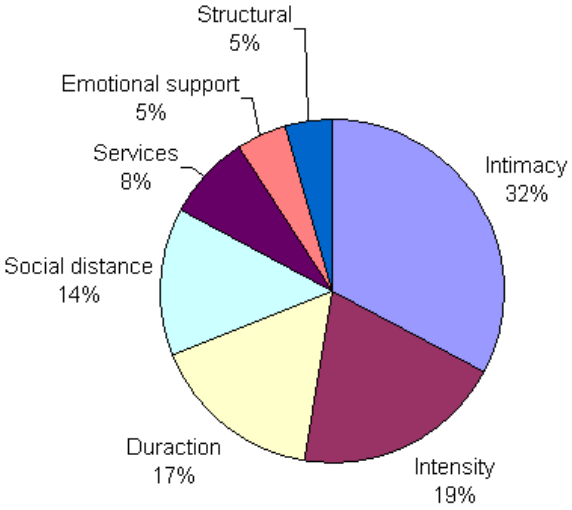

Figure 5. The distribution of the predictive power of the seven tie strength dimensions as part of the How-strong model. Source: [14].

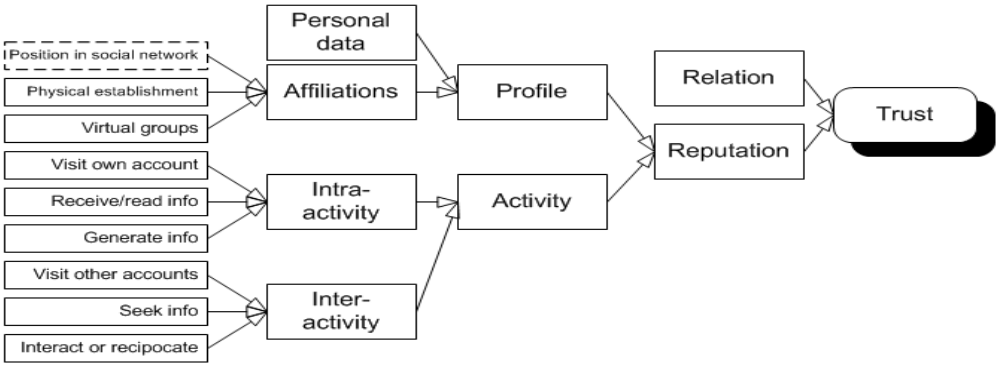

Figure 6. Hierarchical trust metrics model for Facebook

In Figure 5, we can see that the top three strongest dimensions commonly involve about the interactive messaging activities between two users. We therefore organized some activities whose data can be extracted from Facebook as a representative case study of social network, and generalized them into sub-groups of trust factors namely, Profile, Intra- and Inter-activities and other factors, etc. A hierarchical trust metrics model for Facebook is thus established as shown in Figure 6.

We suppose that these factors contribute to the trust with which a user has on another user in Facebook. At the top of the hierarchy, mainly trust is comprised of the relation and the reputation of a person to the user. As discussed in our previous section, reputation is reflected by who he is perceived as by the other people and he did in terms of what message history he left in the social network site. On Facebook, we can further classify the activities as those happened solo, e.g. posting messages on his own wall, and interactions.

Given this hierarchical trust metrics model, we can calculate the tie strength similar to the one in [16] using statistical means over the data collected from Facebook. Most importantly, we want to quantitatively compute the relative weights of the trust factors according to this trust metrics model. Hence in our CF framework, in the calculation of trust T_{ij} between users i and j, the scaling weights over the trust factors can be numerically established, instead of allowing the users to set the values arbitrarily or subjectively.

In order to show as an example of how the relative importance over the trust factors can be calculated, we carried out an experiment using a set of real-life survey data[2]. The survey dataset is taken from The Facebook Project, which is by Jeff Ginger, at the University of Illinois, that provides online resources for researchers in studying Facebook.

The survey dataset was collected in April and May of 2006 and gathered responses from a sample of 124 students (73 undergraduates after filtering). The dataset contains responses to the questions pertaining to perceptions on trust and privacy, meeting people and relationships (identity management), messaging, pictures, and groups on Facebook. The dataset is streamlined to contain only the responses relevant to our hierarchical trust metrics model for Facebook as shown in Table 4. The responses in the datasets which were originally in ordinal data are normalized. Datamining was performed over the pre-processed data by using C4.5 [18] decision tree classification and Apriori association rules.

[2]http://thefacebookproject.com/resource/datasets.html (Go to available files)

Four decision trees are built to classify the samples of data to the groups of trust or otherwise; one group of attributes are used in each decision tree, namely Profile, Privacy, Intra- and Inter-activities. In a nutshell, we want to observe which group of attributes (representing the trust factors) has a greater predictive power and hence influence to the perception of trust by the users. C4.5 builds decision trees from the dataset, using the concept of information entropy that is a measure of the uncertainty associated with a random variable.

Table 4. Attributes used in dataset

Category	Survey questions
Profile	3. How often do you update any aspect of your profile on Facebook 31. Do you list your significant other as such on Facebook 32. College students to display information 33. High school students to display information 34. Faculty and staff to display information 35. Alumni to display information 71. When browsing through profiles will you investigate profiles of people
Intra-activity	4. Investigate view profiles or pictures 5. Investigate view groups or events 6. Investigate view notes or posted items 7. View news feeds personal or general 11. Read wall posts 15. Create groups 16. Create events 17. Post pictures 18. Check out advertisements
Inter-activity	8. Search for people profiles or pictures 9. Search for groups or events 10. Check reply-to or send messages 12. Make or respond to wall-posts 13. Poke others initiate 14. Return pokes reciprocate
Privacy	30. What is your comfort level indicating your relationship status on Facebook 40. Do you think Facebook is invasive or not invasive into your privacy 52. Do you adjust who can see your contact information 53. Do you adjust what information the news feed can publish about you 54. Do you adjust who can see your pictures 56. Do you display your relationship status on Facebook 62. Do you display address or contact information 66. Do you display the interested in category on Facebook 67. Do you feel your Facebook picture is important

Effectively from the quality of the predictive model which is the resultant decision tree formed by a particular group of trust factors, we can tell much the group of trust factors contribute to predicting trust. Therefore by comparing the performance measures of the decision trees which are built by different groups of trust factors, the relative importance (hence the weights) of these groups of trust factors can be quantitatively estimated based on the Facebook survey data.

In this experiment, we deliberately retained the performances of the decision trees in the building process and represented them as Lift Charts [19], one for each group of trust factors. Lift is a measure of the effectiveness of a predictive model calculated as the ratio between the results obtained with and without the predictive model. The cumulative gains which are the curves over the diagonal lines are visual aids for measuring model performance. The diagonal lines are baselines which represent the state in which the model has zero predicting power.

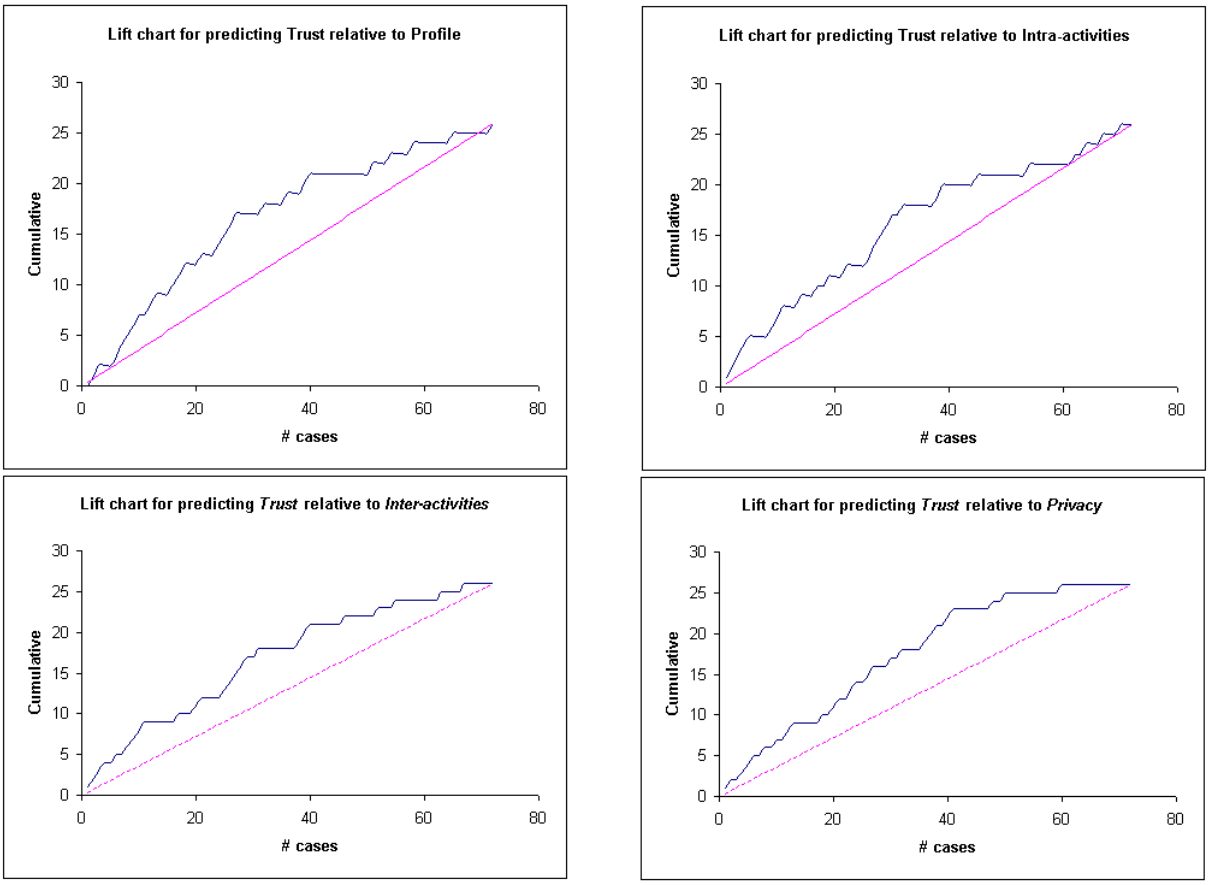

Figure 7. Lift charts of the decision tree models by different groups of factors

The higher the curve of the cumulative gains is, the better the model can predict about the class (which is perception of trust here). In short, the greater the area between the curve of the cumulative gain and the baseline is, the better the model.

Riding on this feature, we simply measure the areas under the lift curves from the baselines for each set of decision trees of trust factors groups. In this experiment, we found the ratios of weights between Profile, Privacy, Intra- and Inter-activities are 0.3265, 0.2449, 0.2041 and 0.2245 respectively. Likewise, the same technique can be applied for measuring the relative weights of any other sets of trust factors. Should the CF framework be changed to other social media than Facebook, different attributes and trust factors would be used.

Data-mining algorithm of Apriori association rules was applied to the same dataset in our experiment. The program used is XLMiner[3]. The results help to verify complimentarily that the decision tree models are consistent with the intuitive concepts about trust on Facebook. Some extracted rules with minimum 90% confidence and insight derived from the decision trees are shown below:

[3] http://www.resample.com/xlminer

About the Profile attributes

- 100% users who post college information, and current faculty information will post alumni information
- 94.12% confidence on rule such that users who trust friends on Facebook and posted alumni information, will post other significant information on FB
- Similar rules regarding posting college students information and current faculty information, will post other significant information on FB have confidence levels of 93% and 90.91%

About the Intra-activities

- In terms of intra-activities, a user who tends to trust friends on FB would have the following actions that are ranked in relevance: read messages on wall, aware about profiles or pictures.
- Those who trust friends on Facebook, investigate profiles and create group, 90% confidence they will create events.

About the Inter activities

- With 80% confidence, the relation is deemed to be trusted when the following three actions are observed: message is replied, wall post is responded and poke reciprocated is returned.

- By the decision tree manifested from the dataset, the most contributing factors of inter-activities to trust on Facebook are listed as follow in importance order: respond to wall posts.

About the Privacy attributes

- Privacy is most related to trust based on the following factors in a sorted order: tendency to investigate on other users' profiles, the user is conscious on setting who can see his profile.
- The following rule shows a positive association with 56.25% confidence level, such that trust is related to privacy when the following things happen: a user is concerned about the comfort.

6. Conclusion

In this paper we proposed a framework for applying collaborative filtering on social network, with a case study of Facebook. Our work is extended from [9] where trust factors are integrated in the calculation. Many researchers in the past studied trust factors in social network and attempted to model some metrics. However one great challenge is to quantify the trust factors especially the scaling weights between them. This is important in trust-aware collaboration filtering as trust factors are considered relatively in MAUT calculation. We took a slightly different approach by using Data-mining, in particular decision tree and its Lift Chart and association rules to estimate the relative importance between the trust factors. Hence the weights of the corresponding trust attributes can be quantitatively estimated, and fit well under our CF framework. Although the sample size of the survey is relatively small, our work demonstrated the concept of estimating trust factors from Facebook data.

7. References

[1] P. Massa, P. Avesani, "Trust-aware recommender systems", *Proceedings of the 2007 ACM conference on Recommender systems (RecSys '07),* October 2007, Minneapolis, USA, pp.17-24.

[2] L. Page, S. Brin, R. Motwani, and T. Winograd, "The pagerank citation ranking: Bringing order to the web", *Technical report*, Stanford, USA, 1998.

[3] J. Golbeck, J. Hendler, and B. Parsia, "Trust networks on the Semantic Web", *In Proceedings of Cooperative Intelligent Agents*, 2003.

[4] C. Ziegler and G. Lausen, "Spreading activation models for trust propagation", *In IEEE International Conference on e-Technology, e-Commerce, and e-Service (EEE'04)*, 2004, pp.83-97.

[5] R. Levien, "Advogato Trust Metric", *PhD thesis*, UC Berkeley, USA, 2003.

[6] Kitisin, S. Neuman, and Clifford, "Reputation-based Trust-Aware Recommender System", *Securecomm and Workshops*, 2006, Baltimore, USA, pp.1-7.

[7] J. Sun, X. Yu, X. Li, and Z. Wu, "Research on Trust-Aware Recommender Model Based on Profile Similarity", *International Symposium on Computational Intelligence and Design (ISCID '08)*, Oct. 2008, Wuhan, pp.154-157.

[8] Z. Wu, X. Yu, J. Sun, "An Improved Trust Metric for Trust-Aware Recommender Systems", *First International Workshop on Education Technology and Computer Science (ETCS '09)*, March 2009, Wuhan, pp.947-951.

[9] P. Kazienko and K. Musiał, "Recommendation Framework for Online Social Networks", *Advances in Web Intelligence and Data Mining*, Springer, Vol. 23, 2006, pp.111-120.

[10] S. Debnath, N. Ganguly, P. Mitra, "Feature Weighting in Content Based Recommendation System using Social Network Analysis", *17th international conference on WWW*, 2008, Beijing, pp.1041-1042.

[11] A. Gursel and S. Sen, "Producing Timely Recommendations From Social Networks Through Targeted Search", *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems - Volume 2*, 2009, Budapest, pp.805-812

[12] P. Massa and B. Bhattacharjee, "Using trust in recommender systems: An experimental analysis", *Second International Conference in Trust Management (iTrust '04)*, Oxford, UK, March 2004, volume 2995 of Lecture Notes in Computer Science, Springer, pp.221–235.

[13] T. Berners-Lee, J. Hendler, and O. Lassila, "The semantic web", *Scientific American*, 2001.

[14] P. Sztompka, "Trust: A Sociological Theory", *Cambridge University Press*, Cambridge, 1999.

[15] C. Dwyer, S. S.R. Hiltz, and K. Passerini, "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace," *Proceedings of the Thirteenth Americas Conference on Informations (AMCIS 2007)*, 2007, pp.339-351.

[16] E. Gilbert, K. Karahalios, "Predicting Tie Strength With Social Media", *Proceedings of the 27th international conference on Human factors in computing systems (CHI '09)*, 2009, Boston, USA, pp.211-220.

[17] J. Golbeck, "Weaving a Web of Trust", *Science Magazine, AAAS,* Vol. 321 (5896), 2008, pp.1640-1641.

[18] J.R. Quinlan, "C4.5: Programs for Machine Learning", *Morgan Kaufmann Publishers*, 1993.

[19] M. Vuk, T. Curk, "ROC Curve, Lift Chart and Calibration Plot", *Metodolo˘ski zvezki*, Vol. 3(1), 2006, pp.89-108.