

INTERPERSONAL TRUST MEASUREMENTS FROM  
SOCIAL INTERACTIONS IN FACEBOOK

by

Xiaoming Li

A thesis submitted in partial fulfillment  
of the requirements for the degree

of

Master of Science

in

Computer Science

MONTANA STATE UNIVERSITY  
Bozeman, Montana

May 2014

©COPYRIGHT

by

Xiaoming Li

2014

All Rights Reserved

## ACKNOWLEDGEMENTS

Please allow me to express my sincere gratitude to Prof. Qing Yang, my mentor and friend, for his continuous support on my study and research, for his great encouragement when I want to give up, for his unselfish help on both my study and personal life, for his tremendous guidance when I felt confused and helpless. Without him, it would not have been possible for me to study in U.S. and keep doing research. He has been and will continue to be a role model for me in the future. I am deeply indebted to Qing for his tremendous love, support and encouragement.

This thesis is dedicated to my past two years.

## TABLE OF CONTENTS

1. INTRODUCTION .....	1
Quantifying Interpersonal Trust.....	1
Online Social Interactions .....	2
Methodology .....	4
Contributions.....	5
Organization of Thesis .....	6
2. BACKGROUND .....	7
Current Approaches on Trust Measurement .....	7
Principle Component Analysis .....	9
Ranking Evaluation Methods.....	10
3. TOWARD TRUST MEASUREMENT BY DATA ANALYSIS .....	12
<i>itrust</i> App .....	12
System Architecture.....	12
System Dataflow .....	14
Participants.....	18
Data Analysis .....	20
Dataset Description.....	21
Features of Social Interaction Data.....	26
Relationship between Interaction and Trust – from a Statistical View .....	28
Statistical Procedures Used.....	28
Summary of Statistical Findings.....	31
Scope of Inference .....	31
4. TRUSTWORTHINESS COMPUTATION .....	32
User Classification .....	32
Data Normalization .....	34
Trustworthiness Ranking .....	39

## TABLE OF CONTENTS - CONTINUED

5. EVALUATION.....	42
Comparison to Ground Truth.....	43
Ranking Accuracy on Most Trustworthy and Untrustworthy Friends.....	47
Ranking Accuracy by Generalized Kendall's Tau.....	48
6. CONCLUSIONS.....	54
REFERENCES CITED.....	55
APPENDICE.....	58
APPENDIX A: User Consent on Using <i>itrust</i> .....	58

## LIST OF TABLES

Table	Page
1. Descriptions of online social interactions in Facebook. ....	21
2. Weight assignment for each factor .....	42

## LIST OF FIGURES

Figure	Page
1. Interactions in Facebook could reflect the interpersonal trust from real world .	4
2. System architecture of <i>itrust</i> .....	13
3. Flowchart of <i>itrust</i> .....	15
4. User consent interface.....	16
5. Authorization interface .....	16
6. JSON format of fetched data.....	17
7. An example of invitation letter .....	18
8. Social network topology among all <i>itrust</i> users.....	19
9. Constitution of <i>itrust</i> users.....	20
10. Distribution of inbox messages.....	22
11. Distribution of interactions of user photos.....	22
12. Distribution of interactions of user albums.....	23
13. Distribution of interactions of tag photos .....	24
14. Distribution of interactions of user's status .....	25
15. Distribution of number of friends .....	26
16. Differences between male and female users on using types of interactions..	27
17. Relationship between number of mutual friends and trust .....	28
18. Fitted values vs. residuals .....	29
19. Normal Q-Q plot of the residuals.....	30
20. Observed (scatter) versus predicted values (the diagonal line) .....	30

## LIST OF FIGURES – CONTINUED

Figure	Page
21. Illustration of the four different types of users .....	33
22. Flowchart of data normalization .....	35
23. Comparison of interaction between Alice-Bob and Alice-David .....	36
24. Examples of user's activity level .....	37
25. An example of data normalization .....	38
26. Normalized interaction matrix .....	38
27. Flowchart of ranking generation .....	40
28. Ranking evaluation interface .....	43
29. Ranking differences among <i>itrust</i> , weighting and ground truth .....	44
30. Ranking differences among <i>itrust</i> , regression and ground truth .....	45
31. Distribution of ranking result by <i>itrust</i> , regression and weighting .....	46
32. <i>itrust</i> accurately discovers highly trustworthy and untrustworthy friends .....	47
33. Illustrations of the Kendall's tau and generalized Kendall's tau methods .....	48
34. Evaluations based on Kendall's tau .....	49
35. Illustration of element weight assignment .....	51
36. Evaluation based on Generalized Kendall's tau .....	52



## ABSTRACT

Interpersonal trust is widely cited as an important component in several network systems such as peer-to-peer (P2P) networks, e-commerce and semantic web. However, there has been less research on measuring interpersonal trust due to the difficulty of collecting data that accurately reflects interpersonal trust. To address this issue, we quantify interpersonal trust by analyzing the social interactions between users and their friends on Facebook. Currently, friends of a user in almost all online social networks (OSN) are indistinguishable, i.e. there is no explicit indication of the strength of trust between a user and her close friends, as opposed to acquaintances. Existing research on estimating interpersonal trust in OSN faces two fundamental problems: the lacks of established dataset and a convincing evaluation method. In this thesis, we consider bidirectional interacting data in OSN to deconstruct a user's social behavior, and apply Principle Component Analysis (PCA) to estimate the interpersonal trust. A Facebook app, *itrust*, is developed to collect interaction data and calculate interpersonal trust. Moreover, we adopt the Kendall's tau and Generalized Kendall's tau methods to evaluate the accuracy of ranking list generated by *itrust*. Results show that *itrust* achieves more accurate interpersonal trust measurements than existing methods.

## INTRODUCTION

Recently, interpersonal trust has been applied in various systems as a key factor in decision making process. Taking e-commerce as an example, the opinions from trustworthy friends strongly influence a user's purchasing decision. By leveraging a buyer's trust to her friends, it is possible to provide her with online reviews she can entirely trust, which would help the buyer to make purchasing decision [1]. Another common example is peer-to-peer (P2P) network, in which a user could determine from which neighbors to download files by evaluating users' trustworthiness [2-4]. Current P2P applications, like Turtle [5] and Tribler [6], are built upon trust information from online social network. Besides, in autonomic computing, trust influences the reliance on automation because people tend to respond to technologies socially [7].

Although interpersonal trust is a very important concept in human's life, there is no formal definition of interpersonal trust. However, most researchers agree that interpersonal trust is "the willingness of accepting vulnerability or risk based on expectations regarding another person's behavior" [8]. Conceptually, trust is also attributable to relationships within and between social individuals or groups (families, friends, communities, organizations, companies and nations). The goal of this work is to find a proper method to measure interpersonal trust.

Quantifying interpersonal trust is a challenging problem because it is difficult to find an appropriate dataset that accurately reflects interpersonal trust. Even if such a dataset were available, accurate estimation of interpersonal trust from the dataset is non-trivial. The first attempt to quantify interpersonal trust is proposed in [9], which tried to estimate trust by analyzing email exchanges between different users. However, email communications are often the reflection of business-related activities, so they are inadequate for analyzing interpersonal trust in more general settings. Social psychologists made use of trust game [10] to measure interpersonal trust. The outcomes from the game, however, cannot be applied widely as the game is conducted within a small group of people.

As the social networks like Facebook can be defined as a set of actors interconnected via relationships [11], we try to dig down further to check the correlation between online social networks and real human lives. People interact with each other in various ways in OSNs, and those interactions can be quantified. So, interpersonal trust could probably be measured by those quantified interactions.

### Online Social Interactions

Thanks to the developments of online social networks (OSN), the richness of data generated within OSN provides unprecedented opportunities for analyzing interpersonal trust. Take Facebook as an example, in April 2014 the total number of Facebook users reached 1.28 billion and 1.23 billion of them are monthly active users [12]. In United States, there are 128 million daily active users, i.e. about 40% of Americans use Facebook every day. Unfortunately, most OSNs do not incorporate interpersonal trust in

the creation and management of relationships. The social role of a friendship was first considered in Google+ by introducing the concept of “circles”. Users can use circles as a way to distinguish their close friends, family and acquaintances. However, this “circles” concept does not quantify interpersonal trust but only the nature of relationships between users.

Since social networks consist of users interconnected via relationships [11], is it possible to measure interpersonal trust from online social interactions? We pose this question because Singh [14] has proved that social interactions had strong effects on interpersonal trust, while interpersonal trust also influences online interactions [15]. On the other hand, Onnela et al. [16] have discovered that there was connection between tie strength and the duration of calls in mobile social networks. Because of these reasons, we pose the hypothesis that interpersonal trust can be inferred from the frequency of social interactions in OSN.

## Methodology

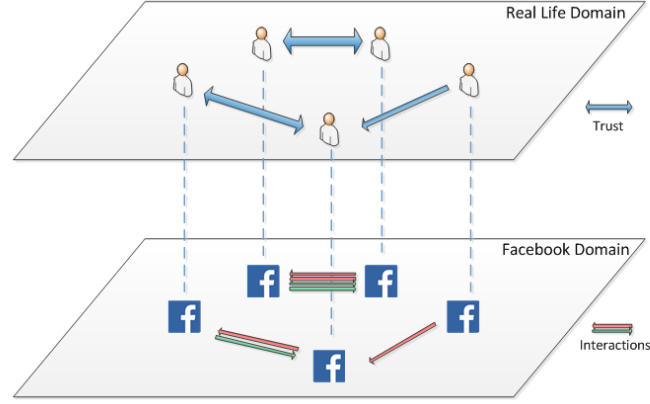


Figure 1. Interactions in Facebook could reflect the interpersonal trust from real world

As mentioned above, OSN like Facebook can be defined as a set of users interconnected via relationships, and each user is the reflection of a person in real life. Unfortunately, friendships in most OSNs are labeled as binary numbers, i.e. a user's close friends and acquaintances show no difference. To address this issue, we propose an innovative approach to quantify interpersonal trust based on online interactions in Facebook. As shown in Figure 1, people connect with each other at various trust levels. Meanwhile, Facebook users connect with each others with different interaction frequencies or times. We might be able to use online interactions in Facebook, e.g. inbox messages, photo tags and comments, to measure the interpersonal trust between users. We develop an app, *itrust*, to collect interaction data between a user and her friends. Then, we normalize those interaction data and apply Principal Component Analysis (PCA) to generate a trust value, which is the estimation of the interpersonal trustworthiness

between the user and her friend. Finally, a ranking list of her friends based on their trust values is returned.

We compare *itrust* to Vedran's weighting method [11] and the regression method adopted by Gilbert [17]. Experimental results show that *itrust* achieves a higher accuracy in estimating interpersonal trust than [11] and [17]. Besides, using the Kendall's tau [18] and generalized Kendall's tau [19] methods, we evaluate friends ranking (based on trust values) and find that *itrust* also outperforms the other approaches.

### Contributions

The contributions of this thesis are as follows:

First, we investigate interpersonal trust by analyzing social interactions in OSN. We normalize users' outgoing data and apply PCA algorithm to generate trust rankings, which show excellent performance in evaluations.

Second, the approach is implemented as a Facebook app, *itrust*, which can accurately rank a user's friends based on their interpersonal trust values, and display the ranking result to the user. *itrust* is open to public and can be reused by any other applications.

Third, we find and prove the correlation between social interactions and interpersonal trust.

Fourth, for the evaluation of trust ranking, we apply the generalized Kendall's tau and we propose a way of assigning weight which specially fits the trust ranking comparison problem.

### Organization of Thesis

The rest of the thesis is organized as follows. In Chapter 2, we discuss the current approaches on trust measurement and background knowledge on principle component analysis which would be applied in *itrust*. Chapter 3 gives the detailed introduction on *itrust* application and analyzes the interaction data collected by *itrust*. Then, we introduce a statistical tool used to demonstrate the existence of correlation between social interaction and trust. Trustworthiness computation is presented in Chapter 4. We apply the PCA approach on trust ranking based on normalized interaction data. Chapter 5 describes the accuracy of *itrust* and makes comparisons to current approaches. In Chapter 6, we discuss the future work and conclude the thesis.

## BACKGROUND

In this chapter, we introduce current approaches on trust measurement, and compare them with our method. Then, brief introductions of PCA and ranking evaluation methods are given, which would be used in our approach.

### Current Approaches on Trust Measurement

Trust measurement has recently attracted many researchers. The common way of measuring trust is through reputation [20], i.e. one can predict the trust of a person by using the former experience of others. Besides, lots of works focus on the propagation of trust [21-24]. Basically, these researches infer trust from known trust, which heavily relies on the existing trust information. However, these trust information are usually not accurate and guaranteed. So, several researchers begin to measure trust directly from the content or evidence on social networks.

Dijiang Huang, etc. [9] tried to measure trust based on the information of email exchange. They analyzed factors including the scale of contacts, email exchanging frequency, relationship catalogs (personal, work, etc.), the degree of contact importance and key words. However, it is not convincing because email communications are usually the reflection of business-related activities, so they are inadequate for analyzing interpersonal trust in more general settings. Besides, the authors faced many problems influencing the measurement performance, e.g. some users chose to keep their contact lists at the mail servers, while others used local server to save their contact lists and letter copies.



Vedran Podobnik [11] attempted to transform online user's social graph from a binary structure to a structure with concrete weights between nodes. They collected 8 factors of social activities, e.g. "list of friends who write on the Facebook's Wall". A specified weight value is assigned to each factor. By calculating the summation of activities with corresponding weights, a friend ranking list would be generated. However, the weight assignment is subjective, i.e. active users can easily get high trust scores, which is not true in reality.

Eric Gilbert identified 74 variables to predict tie strength in online social network [17]. He divided these variables into 7 groups: intensity variables, intimacy variables, duration variables, reciprocal services variables, structural variables, emotional support variables and social distance variables. He used regression to get weight for each variable. The problem of this approach is that, some of the variables, e.g. the number of mutual friends, are proved to be not correlated to trust, which will be introduced in section 3.2.2.

Tencent QQ, the most popular online social tool in China, provides a function called 'intimacy measurement' [25]. Just as the name implies, this function calculates 'intimacy value' between any pair of friends. The calculation is mainly based on three factors. The first factor is 'common background', which checks whether a pair of friends have the same educational or work background, same hometown and the number of common friends. The second factor is 'interactions', which counts the number of social interactions within each other. The third factor is 'common participation', which counts the number of social interactions on common friends' pages. However, this function seems not quite popular because the provided intimacy value is always not accurate or

cannot truly reflect relationships. In our approach, we prove that the factor ‘same background’ like common friends, shows little attributes on relationships. Besides, we consider more interaction factors to measure interpersonal trust.

Compared to earlier works, our approach has the following innovations. First, we measure interpersonal trust based on interactions in Facebook, an appropriate dataset which can better reflects interpersonal trust. Second, we differentiate outgoing data from incoming data, and adopt outgoing data to measure trust. Third, we apply PCA to get an objective trust value instead of subjectively assigning weights on factors.

### Principle Component Analysis

Principal Component Analysis (PCA) is a mathematic tool which can transform a number of correlated variables into a smaller set of uncorrelated variables, called Principle Components (PCs) [26]. Each PC is a particular linear combination of the original variables. During the transformation, most of the information in the original dataset is kept.

In PCA, principle components are extracted by linear transformations from the original variables, the first few PCs contain most of the original information. The number of these PCs, however, would be smaller than the original ones. The first PC will have as much of variability in the data as possible, and each succeeding component will contain the remaining variability.

As a simple method to extract useful information from large dataset, PCA is widely used in many areas in recent years, e.g. face recognition [27], disease prediction

[28], gene expression [29] and so on. Besides, PCA shows good performance in university ranking [30][31], countries ranking[32] and sports team ranking [33]. These scenarios share a common feature that, all variables have positive influences on ranking. For example, in the university ranking, the variables mainly include: number of published articles, number of researchers, size, awards, etc. The bigger the number, the higher the ranking will be.

In this thesis, principle component analysis is applied on trust ranking, which satisfies the application conditions of PCA. As far as we know, this is the first time that PCA is used on trust measurement.

### Ranking Evaluation Methods

For ranking comparison, the concept of ‘rank correlation coefficient’ is introduced to measure the similarities between rankings. The value of such coefficient is usually within  $[-1, 1]$ . Value 1 means the rankings are totally the same, meanwhile value -1 means the rankings are totally reversed. Popular ranking correlation statistical tools include Kendall’s tau and Spearman’s rho.

Kendall’s tau [18] counts the number of all the concordant pairs between two rankings, and mainly calculates the ratio of correctness. It is defined as:

$$\tau = \frac{(\text{number of concordant pairs}) - (\text{number of discordant pairs})}{\frac{1}{2}n(n-1)} \quad (1)$$

Where  $n$  is the number of elements in the rankings. If the two ranking lists are independent, the expectation of the result  $\tau$  should be 0.

As for the spearman correlation, it first creates ranking list by the raw score (usually provided by user), and calculate the differences between the ranks for each observation  $d$ , then  $\rho$  is given by:

$$\rho = 1 - \frac{6 \sum d_i^2}{n(n^2 - 1)} \quad (2)$$

Unlike general ranking comparisons, trust ranking comparison is more complicated. In trust ranking, the importance of each pair-wise disagreement is different. In this thesis, a revised version of Kendall's tau is adopted to evaluate the accuracy of trust ranking.

## TOWARD TRUST MEASUREMENT BY DATA ANALYSIS

How many types of social interactions are there in OSN? What type of interactions reflects trust? To answer these two questions, we first collect all available interaction data in Facebook. Then, we analyze the features of different types of interactions and their impacts on interpersonal trust.

### *itrust* App

Facebook provides an API for developers to collect any kind of data from any user (if permitted). On this basis, we developed an application called *itrust* to collect data on users' interactions and generate a ranking of the trustworthiness of a user's friends. When a user logs into *itrust*, *itrust* will ask her to authorize permissions to access her public profile, friend list, messages, news feed, relationships, status updates, and photos. After authorization, *itrust* begins to collect social interaction data. Due to privacy concerns, *itrust* does not save any details like contents of inbox messages or comments, but only counts the occurrences of these interactions. Based on such interaction data, *itrust* generates a friend ranking list and shows it to the user.

### System Architecture

*itrust* contains three tiers: presentation tier, logic tier and data tier. The system architecture is shown in Figure 2. The presentation tier interacts with users, i.e. asks users to authorize permissions and display ranking list to users. In Facebook, there is no direct way of evaluating the accuracy of the interpersonal trustworthiness computed by *itrust*.

Therefore, we develop the ranking evaluation module to allow a user to input her opinion about her friends' trustworthiness, which is considered as the ground truth. The logic tier performs data normalization and interpersonal trustworthiness calculation, which will be elaborated in chapter 4.

The data tier stores interaction counts obtained from Facebook and friends trustworthiness results computed by the ranking calculation module. Such trustworthiness information could be used by external applications, e.g. P2P program to determine from which peer to download files.

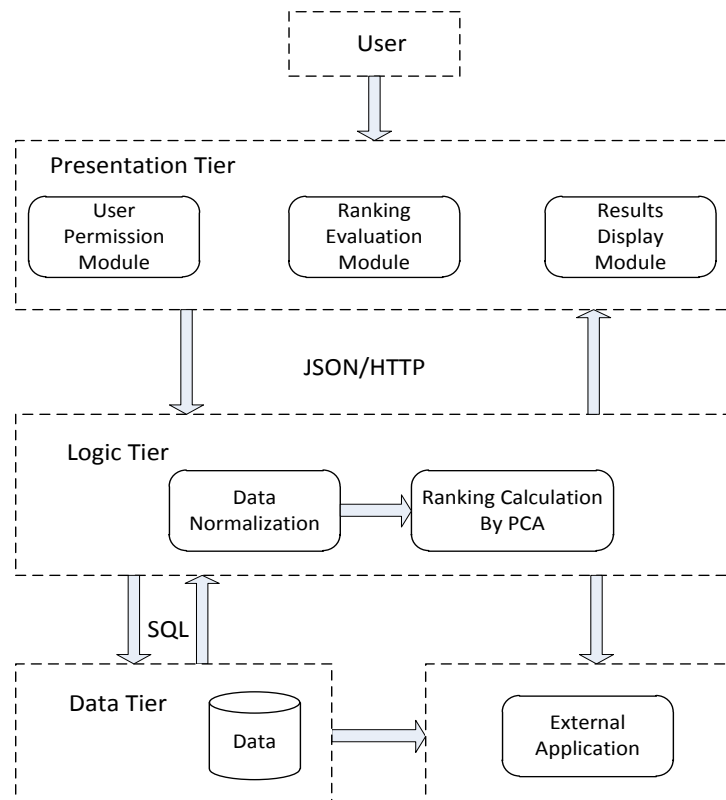


Figure 2. System architecture of *itrust*

If users do not revoke their permission authorizations, *itrust* continuously monitors the users' interaction data, and thus address the temporal dynamics on interpersonal trust relationships. In other word, *itrust* provides a real-time measurement of interpersonal trust between users in Facebook.

### System Dataflow

Data flow diagram of *itrust* is shown in Figure 3. The major processes of *itrust* are: login, authorization, data collection and result display. Besides those regular processes, *itrust* also asks users to improve the *itrust* performance by providing ground truth results and invite friends to use *itrust*.

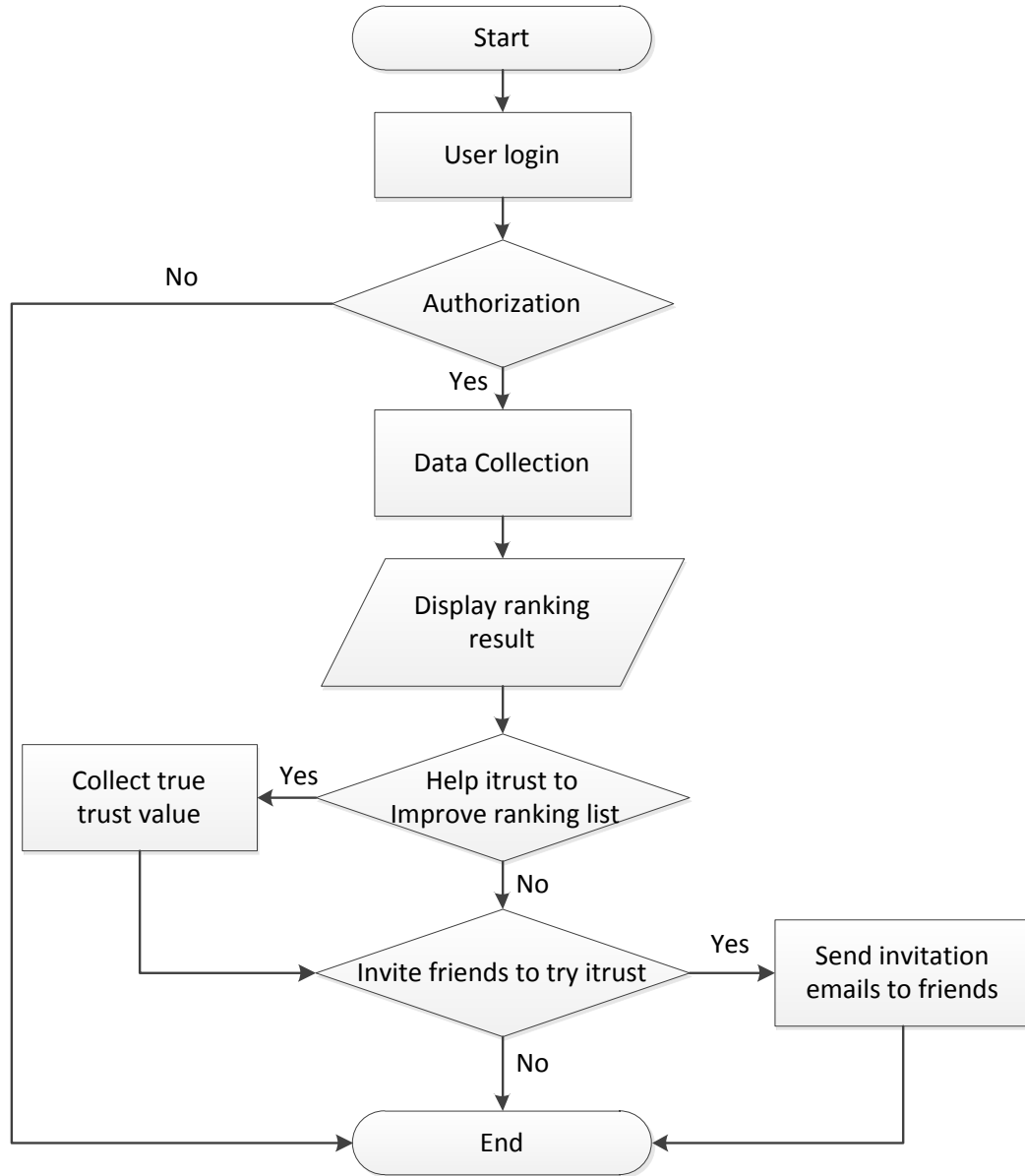


Figure 3. Flowchart of *itrust*

First, when a user logs into *itrust*, a consent page will be shown up, as seen in Figure 4. The details of the consent can be found in the Appendix.



SUBJECT CONSENT FORM FOR PARTICIPATION IN HUMAN RESEARCH AT MONTANA STATE UNIVERSITY

Title: Understanding Interpersonal Trust based on Social Network User Interactions

You are being asked to participate in a research study of understanding interpersonal trust based on social network user interactions. People tend to interact intensely with a small subset of friends, carrying out a social grooming in order to maintain and nurture strong and trustful ties. This study will help us obtain a better understanding of how interactions between online social network users can reflect the interpersonal trust between them.

You have been identified as a possible subject because either you have at least 2-month experience in using Facebook, or one of your Facebook friends recommends you. If you agree to participate, you will be asked to login to your Facebook account and go to the i-trust app. The whole experiment should be finished within 2 minutes. Participation is voluntary!

After logging into Facebook.com and clicking the i-trust app, you need to wait less than 2 minutes to allow the i-trust app to collect your interaction data. The time i-trust takes to collect data depends on how frequently you interacted with your friends, and how many friends you have. Interaction data being collected include the numbers of inbox messages, photo comments, photo likes, album comments, album likes, tags, **tagged**, tag-photo comments, tag-photo likes, co-tags, status likes, and status comments. Data collected in this experiment is retrieved for aggregated evaluation, and original data/text will not be stored anywhere. User names will be coded, so it is impossible to track an user's ID based the stored data. An example of data entry stored on the MSU server looks like:

name	friendname	inbox	photo comments	photo likes	album comments	album likes	tag	tagged	photo comments	photo likes	co tags	status comments	status likes
al2d	al646843	0	3	1	0	2	1	2	1	2	0	0	3



Data collected in this experiment will be kept confidential on MSU servers with access restricted to investigators. Data collected in the experiment will be aggregated and made public without links to your personal information.

☒ I agree with the conditions.


GO! EXIT

Figure 4. User consent interface

After login, *itrust* will ask the user to authorize permissions. The required permissions are shown in Figure 5. Even though we only make use of interaction data, some static information like gender and education history are still collected, in order to analyze the features of *itrust* users.

**iTrust** will receive the following info: your **public profile**, friend list, custom friends lists, messages, News Feed, relationships, birthday, work history, status updates, education history, hometown, current city, photos and personal description and your friends' relationships, birthdays, work histories, status updates, education histories, hometowns, current cities, photos and personal descriptions.

 This does not let the app post to Facebook.

Cancel Okay

Figure 5. Authorization interface

Then, *itrust* begins to collect data from the user's profile, which is described in JSON format. Figure 6 shows an example of a tag-photo data structure. The tag and like information can be found by searching the objects 'tags' and 'likes' in JSON. In this example shown in Figure 6, two people are tagged in the photo, and the JSON file has two matching records in the 'tag' property, i.e. the names and ids of the tagged users. By tracing those ids, detailed information of those tagged users can be found.

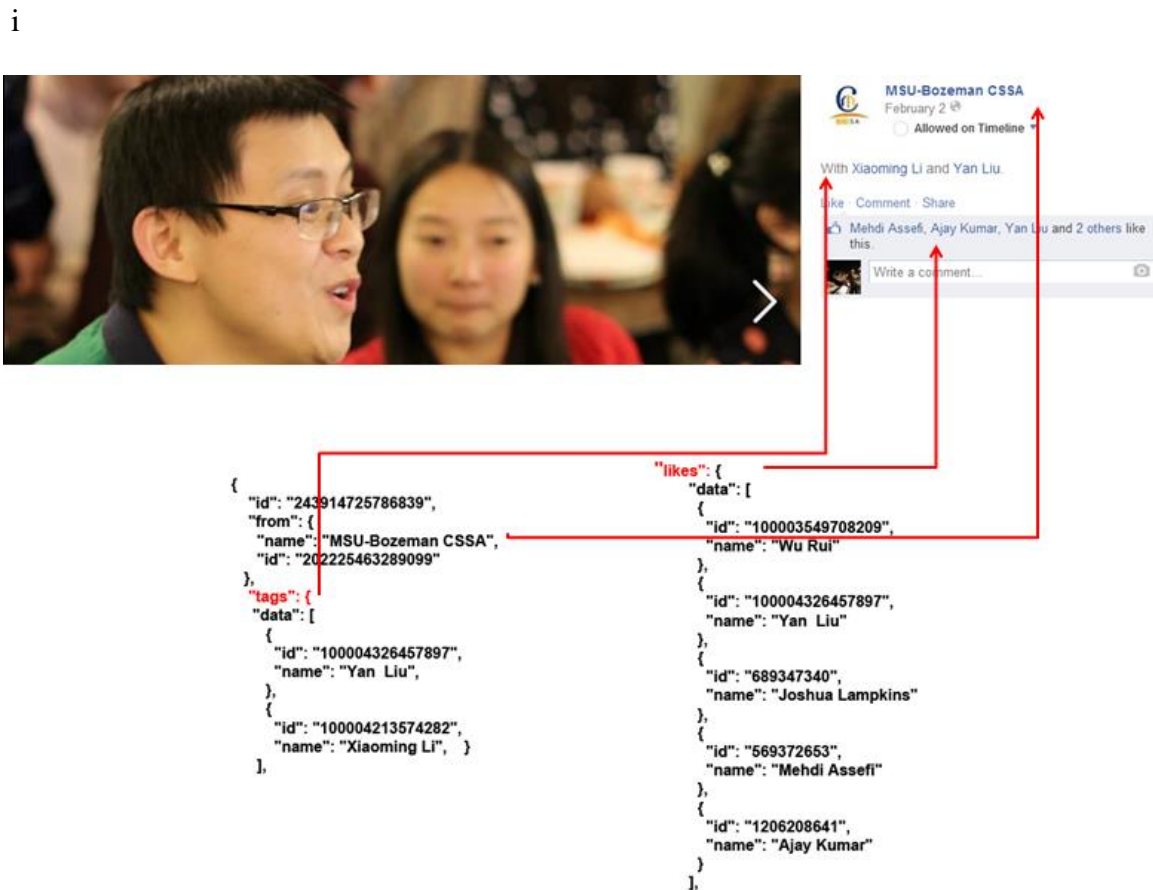


Figure 6. JSON format of fetched data

## Participants

Participants are diverse in races, ages, majors and working experiences, and the “social network” composed of those participants is representative. Initially, several users are specifically selected based on their backgrounds, e.g. age, major and nationality. In order to involve more people in participation, a tricky setting is made that once a user logs into *itrust*, *itrust* will request her to send invitation emails to her friends. Besides, abundant prizes are provided to encourage participation. Figure 7 shows an example of the invitation letter.

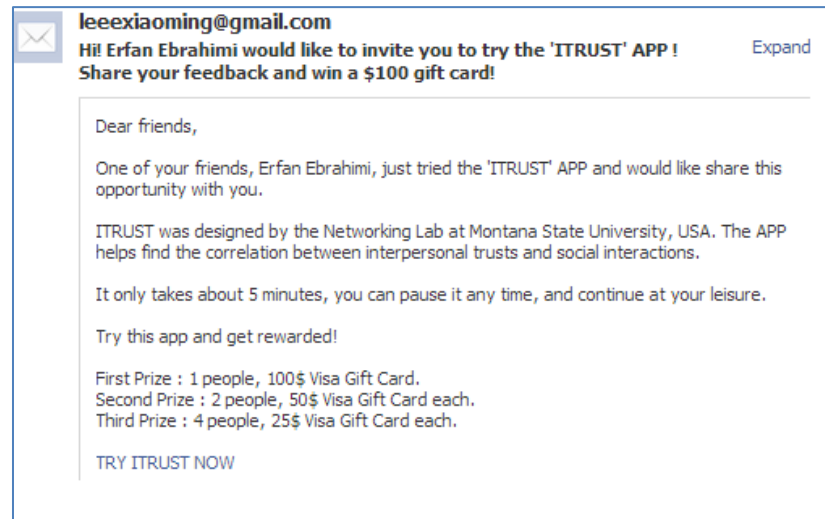


Figure 7. An example of invitation letter

Till 03/25/14, there is a total of 59 participants use *itrust*, a social network consist of those participants is generated, and the network topology is shown in Figure 8. The average node degree is 4, and network exhibits a relatively small, which indicates the network is close and dense.

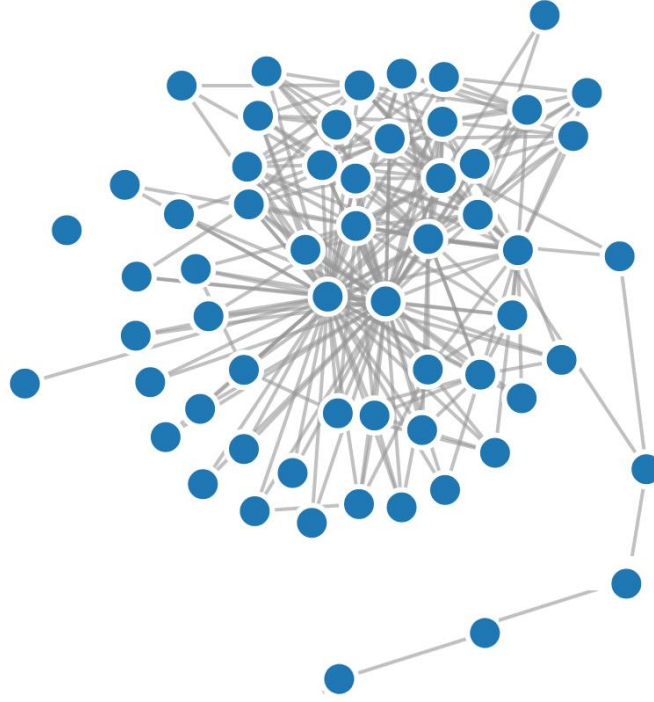


Figure 8. Social network topology among all *itrust* users

Details of *itrust* users are shown in Figure 9. We can see that these users are diverse in race, age, educational background and nationality, so that our findings are applicable in a more general setting. However, the constitution of *itrust* users still shows a unique characteristic. As shown in Figure 9, users with graduate education background take a large proportion. Besides, almost half of the users are Iranian, which doesn't match up to the real proportion of Facebook users.

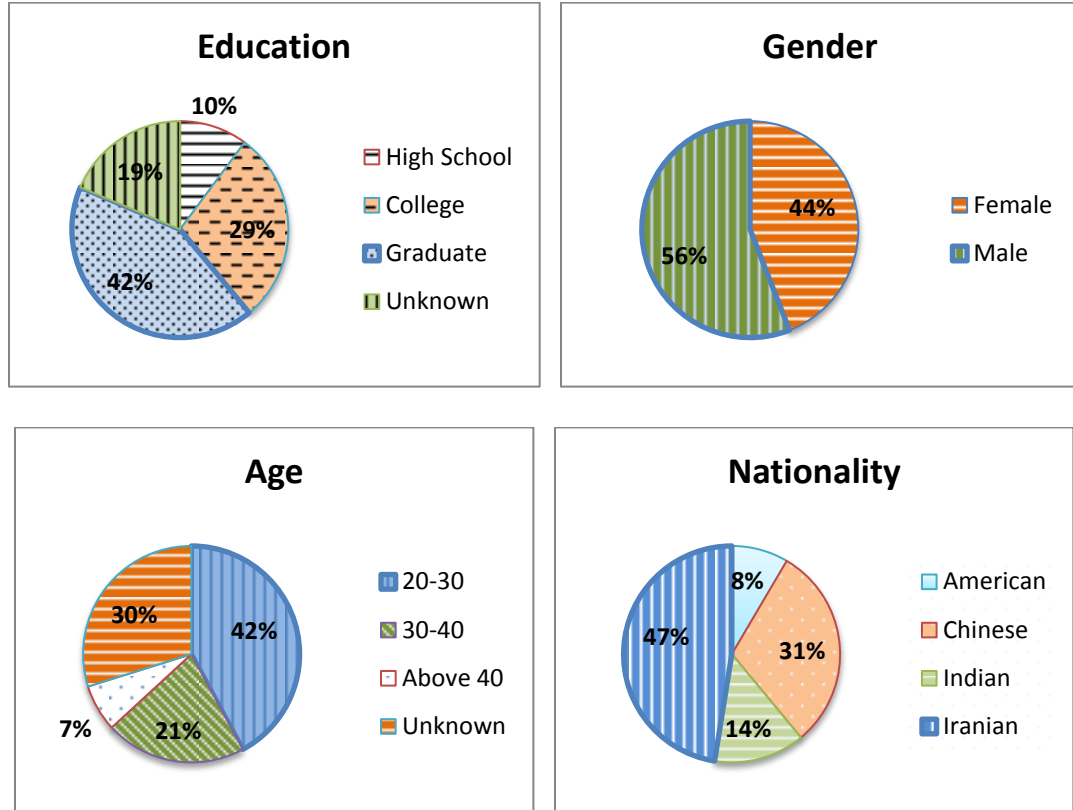


Figure 9. Constitution of *itrust* users

### Data Analysis

*itrust* can save all social activity data of users, however, due to privacy issues, *itrust* only save the number of interactions instead of the contents. After analyzing those interaction counts, several insights are discovered. Besides, correlation between interaction and trust are found from on the dataset.

### Dataset Description

As mentioned above, *itrust* only saves the number of interactions. For each user, we collected twelve different types of interaction data, and obtained a total of 15,158 records. The collected interaction data include: inbox messages, photo comments, photo likes, album comments, album likes, tag photos, tagged photos, tagged photo comments, tagged photo likes, tag-together photos, status comments, and status likes. Table 1 describes the details of each type of interactions.

Table 1. Descriptions of online social interactions in Facebook

Symbol	Factor	Description
$IM_{ij}$	Inbox Messages	The number of inbox messages that $i$ received from $j$
$PC_{ij}$	Photo Comments	The number of comments that $j$ left on the photos of $i$
$PL_{ij}$	Photo Likes	The number of likes that $j$ left on the photos of $i$
$AC_{ij}$	Album Comments	The number of comments that $j$ left on the albums of $i$
$AL_{ij}$	Album Likes	The number of likes that $j$ left on the albums of $i$
$TP_{ij}$	Tag Photos	The number of photos that $j$ was tagged in the photos of $i$
$PT_{ij}$	Photos Tagged	The number of photos that $i$ was tagged in the photos of $j$
$TC_{ij}$	Tag Photo Comments	The number of comments that $j$ left on the tag-photos of $i$
$TL_{ij}$	Tag Photo Likes	The number of likes that $j$ left on the tag-photos of $i$
$CT_{ij}$	Co-tag	The number of photos that $i$ and $j$ were tagged together
$SC_{ij}$	Status Comments	The number of comments that $j$ left on the status of $i$
$SL_{ij}$	Status Likes	The number of likes that $j$ left on the status of $i$

For each user, the average number of each interaction is calculated and showed in Figure 10 to Figure 14. Facebook users tend to use instant message to interact with their friends. As shown in Figure 10, 50% users send more than 200 messages averagely to each of their friends. The average number of inbox messages ranges from 6 to 1400.

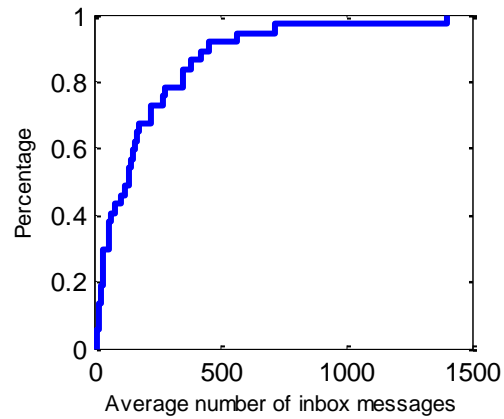


Figure 10. Distribution of inbox messages

Publishing photos is one of the primary functions of Facebook. Basically, users have two ways to interact with a photo publisher, leaving ‘like’ or ‘comment’ on the photo. The average number of photo comments or likes is smaller than 8. Compared to ‘inbox message’, even though interactions about photos are lower by two orders of magnitude, they are still not ignorable as they play an important role in social interaction.

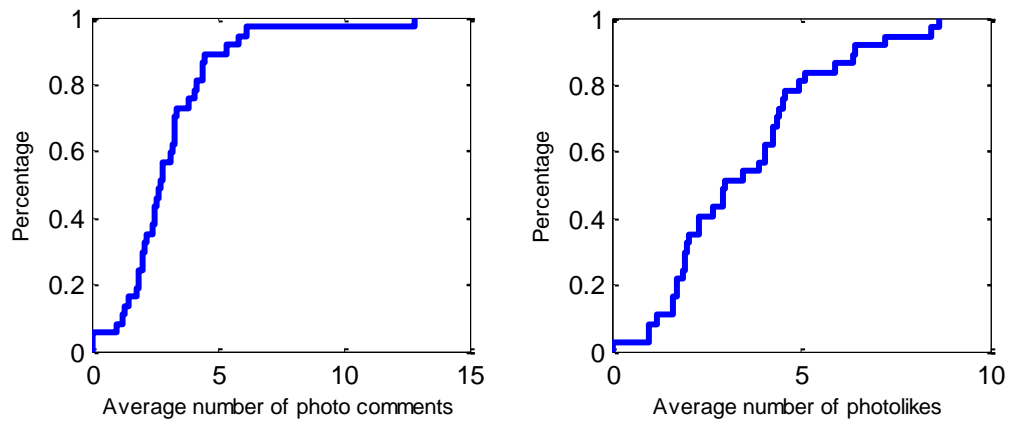


Figure 11. Distribution of interactions of user photos

Meanwhile, the number of interactions of user's albums is relatively small, mainly because the amount of albums user create is usually very small. As shown in Figure 12, the range of album interactions is from 0 to 3.

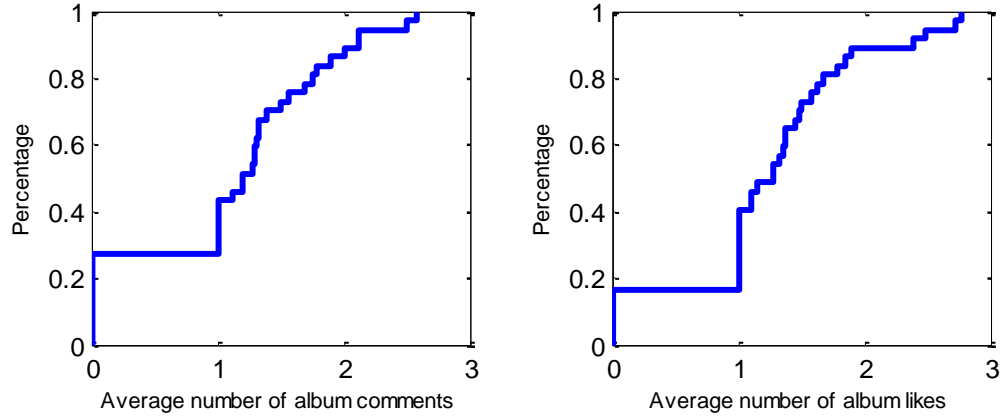


Figure 12. Distribution of interactions of user albums

In Facebook, 'Photos of you' and 'your photos' are different. 'your photos' contains photos a user ('you') published, meanwhile 'photo of you' contains photos where a user ('you') is tagged. We count the time that a user is tagged (which equals the number of his tag photos) and the user tags others, and the comments or likes left on those photos. Figure13 shows that these interactions have the same order of magnitude as user's photos, which is great for analysis.



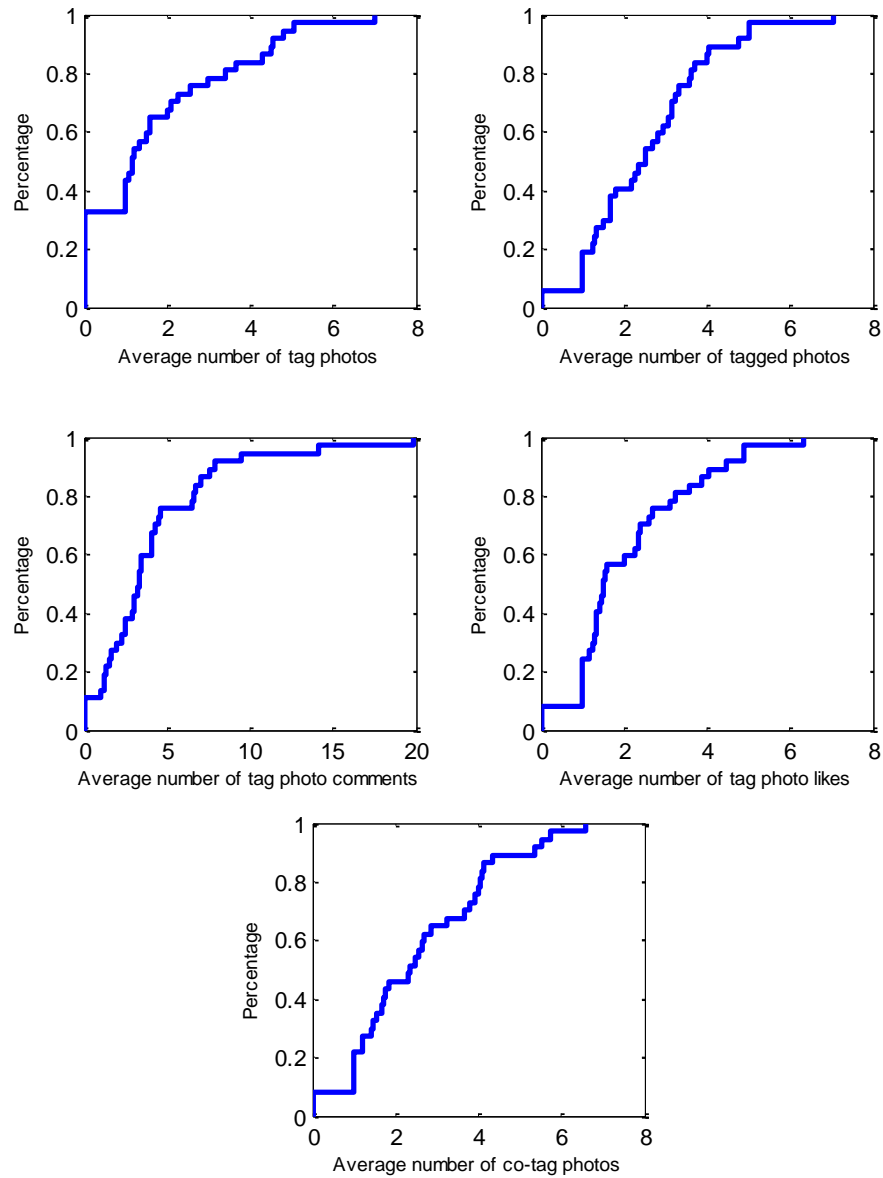


Figure 13. Distribution of interactions of tag photos(usually belong to a user's friends)

Another important function that Facebook provides is publishing status, so that a user's friends can interact by leaving comments or likes. The distributions of interactions of user's status are shown in Figure 14.

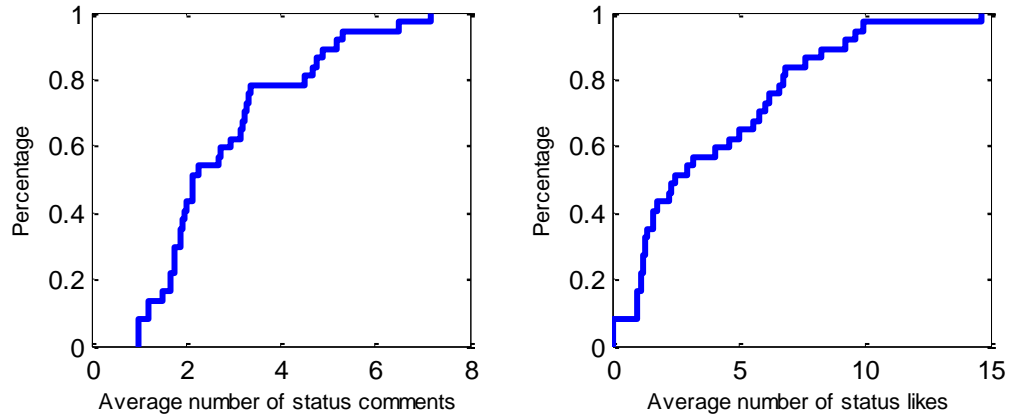


Figure 14. Distribution of interactions of user's status

From the analysis above, we can conclude that, those interactions have different order of magnitude. Even though the number of some interactions is quite small, they are big enough for analysis and we cannot ignore them because they present important social interactions in Facebook.

Meanwhile, some users have lots of friends while others don't. In our dataset, the maximum number of friends that a user has is 1081, while the minimum is 6. The cumulative distribution of which is shown in Figure 15. The median number of friends is around 230, which corresponds with the fact that the median number of friends is 200 in Facebook.

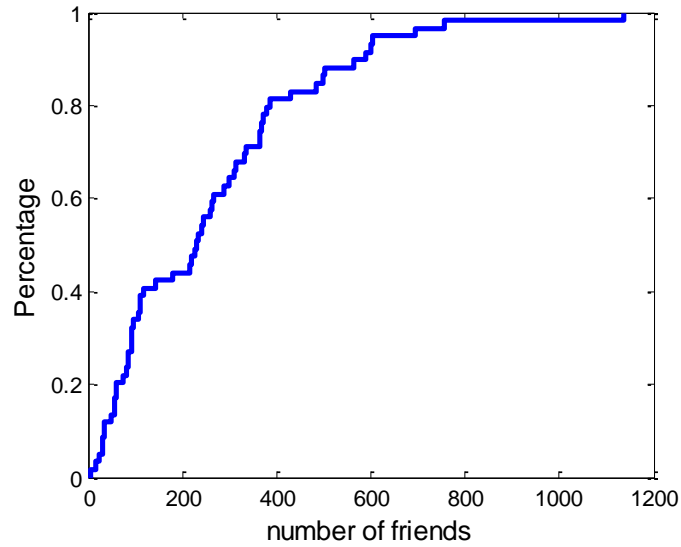


Figure 15. Distribution of number of friends

#### Features of Social Interaction Data

Through data analysis, we find that female users tend to interact with their friends by more types of interactions. Besides, we find some factors like number of mutual friends, don't show significant impact on trust, so we only adopt interaction data to measure trust.

Differentiation between Male and Female Users. It is common said that male and female have different habits of using OSN. *itrust* users are divided into 13 groups by the cumulative number of interactions (0-12), and we try to analyze the friend classifications for each individual user. We found that one main factor is the gender. From Figure 16 we can see that female users always interact with their friends by more types of interactions.

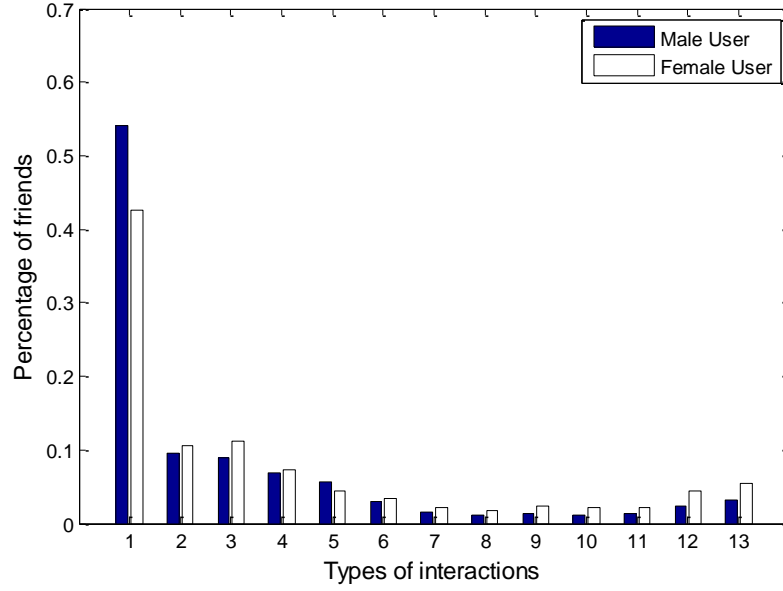


Figure 16. Differences between male and female users on using types of interactions

Correlation between Potential Influent Factors and Trust. We also find that interaction data has more correlations with trust than other types of data. Besides interaction data, there are some other factors like the number of mutual friends, age differences or education differences, which are used in previous research and some of them are treated as important factors. Based on the 785 data entries with trust information provided by users, we analyze the correlation between 22 potential factors with trust by linear regression, the result shows that 12 interaction factors among 22 have bigger correlation coefficient, which is one of the reasons that we use interaction data to predict trust. Figure 17 shows the relationship between the number of mutual friends and the trust of a user, the trust score doesn't go up with the increased number of mutual friends. This is because, many users are connected just by mutual friends, but they are not

familiar with each others. Based on the above observations, we prepare to use interaction data to predict interpersonal trust.

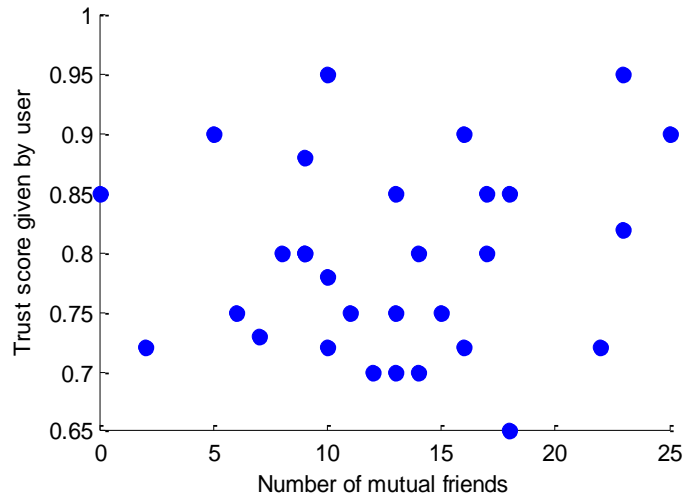


Figure 17. Relationship between number of mutual friends and trust

### Relationship between Interaction and Trust – from a Statistical View

Before we make attempt to measure trust based on interaction data, a statistical tool is used to show the correlation between interaction data and trust.

### Statistical Procedures Used

Linear regression model is applied to check whether there exists correlation between interaction data and trust. Two preconditions should be checked before correlation calculation: dataset must follow normal distribution and has constant variance.

Residual plots in Figure 18 and Figure 19 (Figure 18: Fitted values vs. residuals; Figure 19: Normal Q-Q plot of the residuals on right) demonstrate that residuals have

constant variance, with the residuals scattered randomly around zero, and residuals shows normal distribution. Such observations indicate the correctness of normality and equal variance of the dataset. Figure 20 shows the plot of observed (scatter) versus predicted values (the diagonal line). The points are symmetrically distributed around the line which indicates the correctness of linearity. Possible violations of independence include that, a big portion of the participants are author's friends. They are probably similar on social behavior on Facebook because they have the same background like education, so they may not represent well for a larger population. However, the similarity of social behaviors cannot be proved anyway, so the violation is not considered to be severe.

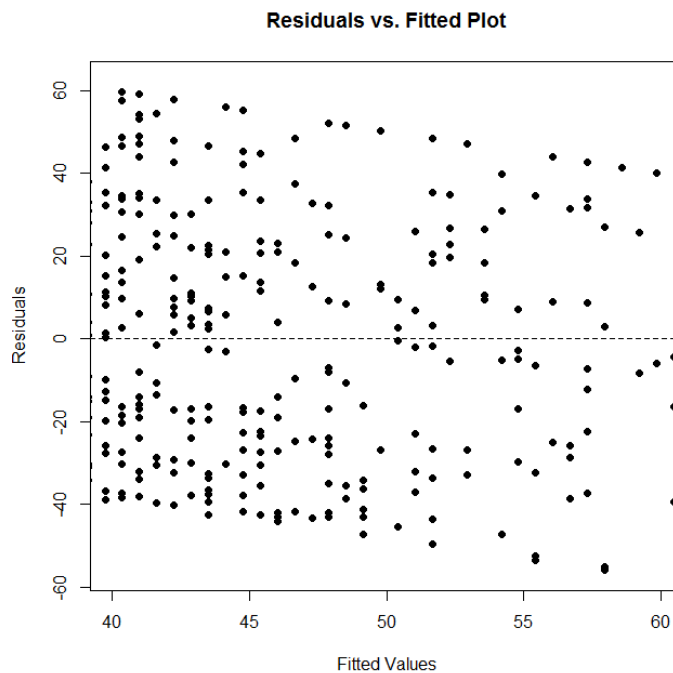


Figure 18. Fitted values vs. residuals

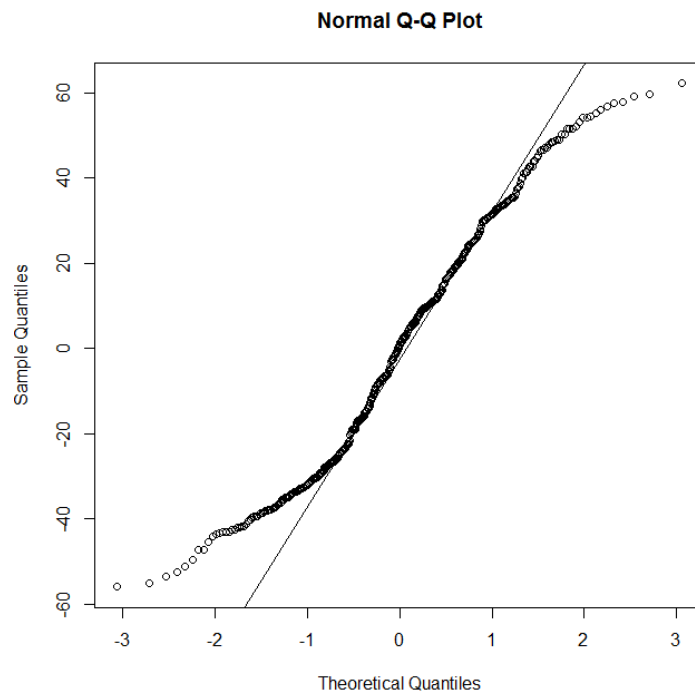


Figure 19. Normal Q-Q plot of the residuals

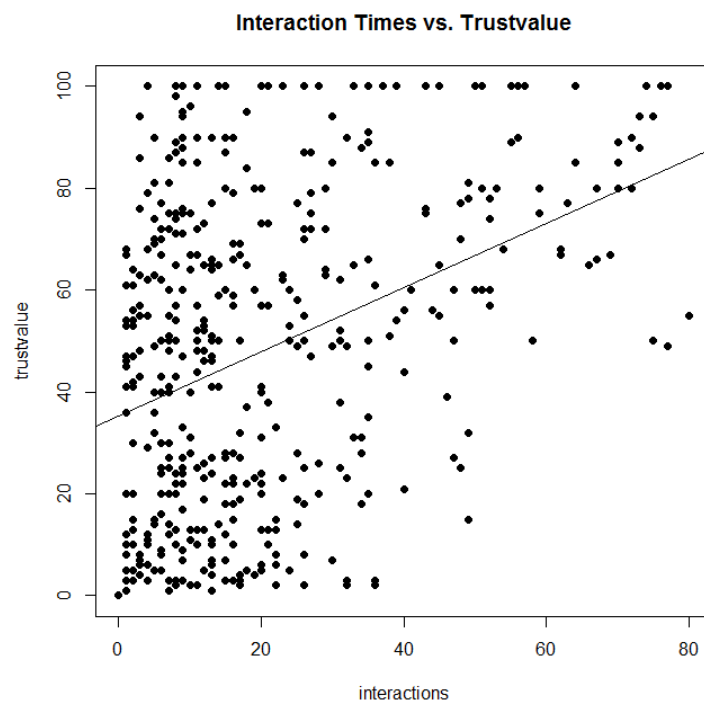


Figure 20. Observed (scatter) versus predicted values (the diagonal line)

### Summary of Statistical Findings

There are convincing evidences supporting the correlations between interaction and trust values (two-sided p-value  $< 0.0001$  from  $f\text{-stat}=294.1$  on 1 and 442 d.f.). One unit increase in interaction times is associated with an estimated 0.62 units increase in the mean trust value, with an associated 95% Confidence Interval from 0.48 to 0.77 units. Based on this observation, it is convincible to use interaction data to measure interpersonal trust.

### Scope of Inference

The participants are not randomly selected from any population; therefore, extending any inference to any larger population is speculative. Also, there is no random assignment of interactions to trust values; therefore, no causal connection between interaction and trust value can be established from the study.



## TRUSTWORTHINESS COMPUTATION

As we are interested in the trustworthiness of friends from a user's perspective, *itrust* uses users' outgoing data to infer their friends' trustworthiness. However, outgoing interactions cannot be used directly because the amount of a user's outgoing interactions is not only determined by her friends' trustworthiness, but also influenced by her friends' levels of activity. Due to social grooming, a user tends to interact more with active friends than inactive ones. Therefore, a user's outgoing interaction data need to be normalized based on how active her friends are. After normalization, principle component analysis is applied to generate trust ranking.

### User Classification

After analyzing each type of data, we discover five characteristics of the interaction data in Facebook. First, large variance exists in each type of interaction data. For example, the average number of messages sent by a user is 9.54, while the maximum is 4214. The average number of status like is 0.35 but the maximum is 53. Second, different interactions reflect interpersonal trust in different ways. For example, a user could be tagged by her friend A in photos 5 times, and she might also receive 5 status likes from another friend B. Although the numbers of interactions with A and B are the same, the user may trust A more than B. Third, several interactions show high level of correlation between each other. For instance, the interactions 'tagged photo comments' and 'tagged photo likes' are highly correlated with the number of the tagged photos.

Fourth, social interactions in Facebook are directional, so is the interpersonal trust. We define the data sent by a user in Facebook as her outgoing interactions, the data she receives as her incoming interactions. Fifth, the amounts of interaction data generated by different users are different, so we classify Facebook users into four categories based on how active they are.

**Active User:** Users who often publish contents (status updates, photos, etc.) and often interact with others.

**Actor User:** Users who often publish contents, but seldom interact with others.

**Audience User:** Users who seldom publish contents, but often interact with others.

**Inactive User:** Users who seldom publish contents, or interact with others.

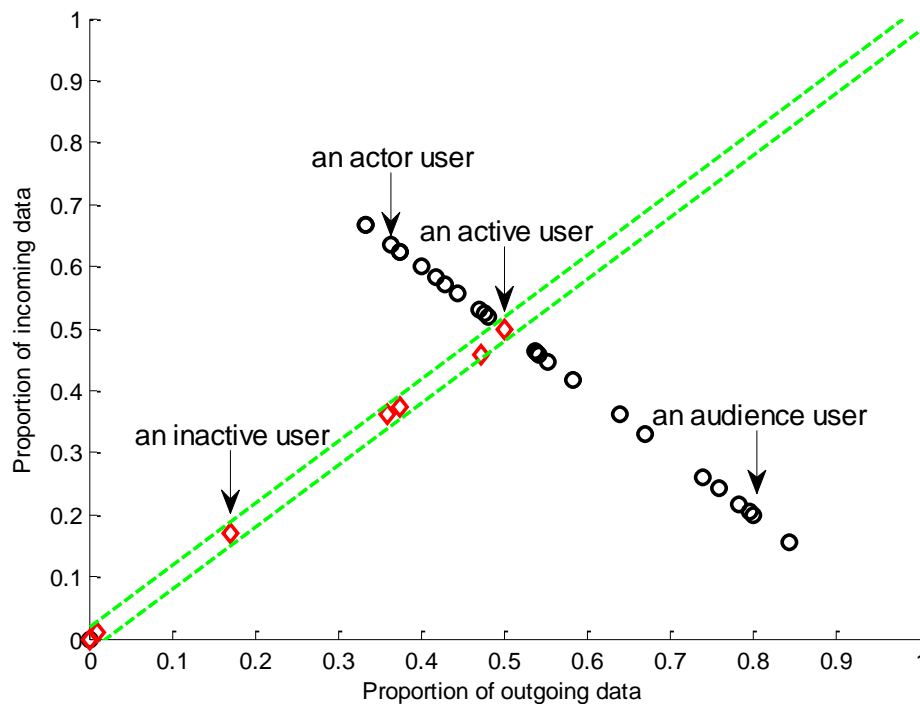


Figure 21. Illustration of the four different types of users

By checking the proportions of incoming and outgoing data, we can easily identify actor and audience users. For example, an actor user often publishes contents but seldom interacts with others, so she tends to have more incoming data (e.g. receiving comments) but less outgoing data. On the other hand, an audience user would have less incoming data but more outgoing ones. Although both active and inactive users would have similar proportions of incoming and outgoing data, the total amount of interactions of active users should be much greater than that of inactive ones.

We randomly select 32 users and display the proportions of their incoming and outgoing data in Figure 21. From this figure, we can clearly see that there are actor and audience users, depicted as circles. In Figure 21, we use diamonds to indicate the users with similar proportions of incoming and outgoing data. We treat the user with the highest amount of interaction data as an active user, and then normalize the other users' proportions of incoming and outgoing data. We can see there are some inactive users at the lower-left corner of Figure 21.

In summary, the interaction data in Facebook are disperse, diverse, correlated, directional and user-dependent; therefore, they must be processed before being used to infer the interpersonal trust information.

### Data Normalization

For every friend of the user, we first need to measure how active the friend is. Suppose the friend is A, we use the average number of A's incoming data to indicate how active A is. Specifically, we use the average count of incoming interaction data (of twelve

different types) received from all A's friends to describe A's level of activity. Such friends' levels of activity information help *itrust* eliminate the problem that large amount of outgoing data are generated when the user is interacting with untrustworthy but active users. Specifically, we normalize the user's outgoing data by dividing each type of her interaction data by each of her friend's level of activity, respectively. Figure 22 shows the flowchart of data normalization, where a user's friends' incoming data are used to normalize user's outgoing data.

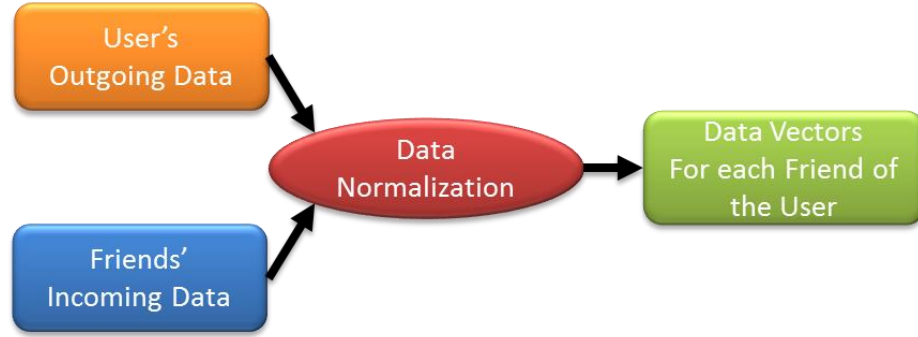


Figure 22. Flowchart of data normalization

We define that, for a user  $i$ , user  $j$  is a friend of  $i$ ,  $F_i$  is the set of  $i$ 's friends, so  $j \in F_i$ , then we have:

$r_{ij}^k$ : the number of interaction of type  $k$  that  $i$  received from  $j$ ;

$s_{ij}^k$ : the number of interaction of type  $k$  that  $i$  sent to  $j$ .

Based on the definition, we have

$$r_{ij}^k = s_{ji}^k \quad (3)$$

The average number of interaction  $k$  that  $i$  received from all her friends is:

$$\overline{r_i^k} = \frac{\sum r_{ij}^k}{|F_i|} \quad (4)$$

$\overline{r_i^k}$  is defined as user  $i$ 's activity level on interaction  $k$ . For any  $m \in F_i$ ,  $m$ 's outgoing data sent to  $i$  on interaction  $k$  is  $s_{mi}^k$ , which is normalized by user  $i$ 's activity level:

$$\widetilde{s_{mi}^k} = \frac{s_{mi}^k}{\overline{r_i^k}} \quad (5)$$

An example is shown in Figure 23. Bob and David are Alice's friends, and the trust from Alice to Bob/David is going to be measured. Arrows represent different types of interactions, and the numbers on arrows denote the number of interactions. As shown in the figure, these are three types of interactions between Alice and Bob, number of which are 6, 15 and 2, respectively. And the numbers of interactions are 2, 5 and 1 between Alice and David.

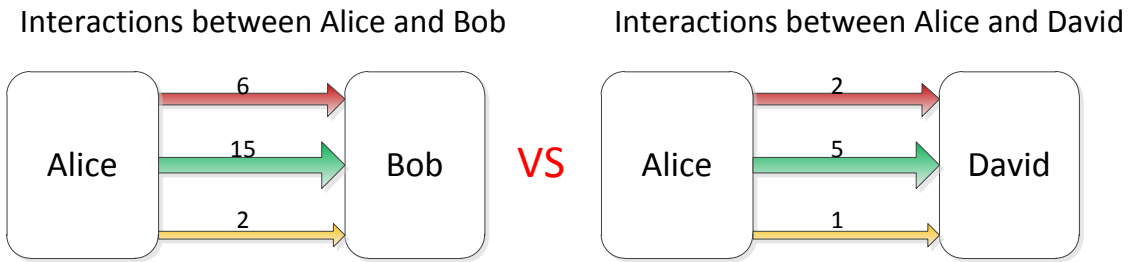


Figure 23. Comparison of interaction between Alice-Bob and Alice-David

Alice has more interactions with Bob than David, so Alice should trust Bob more. However, the truth might be that Bob is an active user and David is an inactive user.

Even Alice trusts David more, her interactions with David still seem to be small. So the activity level of Bob and David must be taken into account.

A user's activity level is measured by averaging the count of incoming interactions by types from All user's friends. Figure 24 shows the activity levels of Bob and David, which are (3, 15, 2) and (1, 1, 1). It means that, compared to David, Bob is more active in using Facebook, e.g. he publishes status and photos a lot more, so his friends have more opportunities to interact with him.

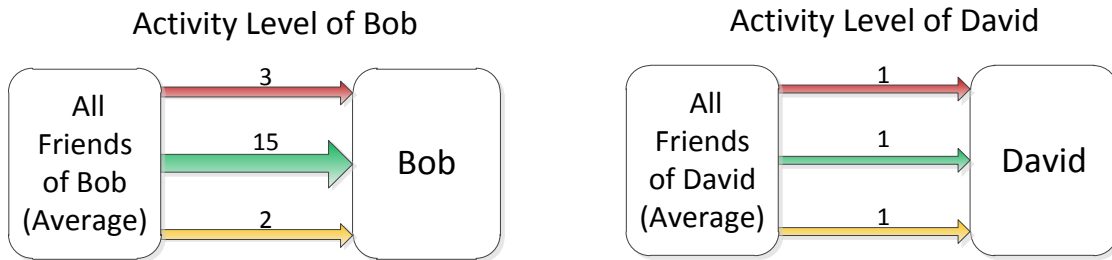


Figure 24. Examples of user's activity level

Figure 25 shows the normalization of interactions between Alice and Bob. That is, we divide each type of Alice's interaction data by Bob's level of activity, respectively. Finally, we get the normalized interaction data between Alice and Bob, which is a vector shown as  $(6/3, 15/15, 2/2)$ , which is (2, 1, 1). And interactions vector between Alice and David is (2, 5, 1).

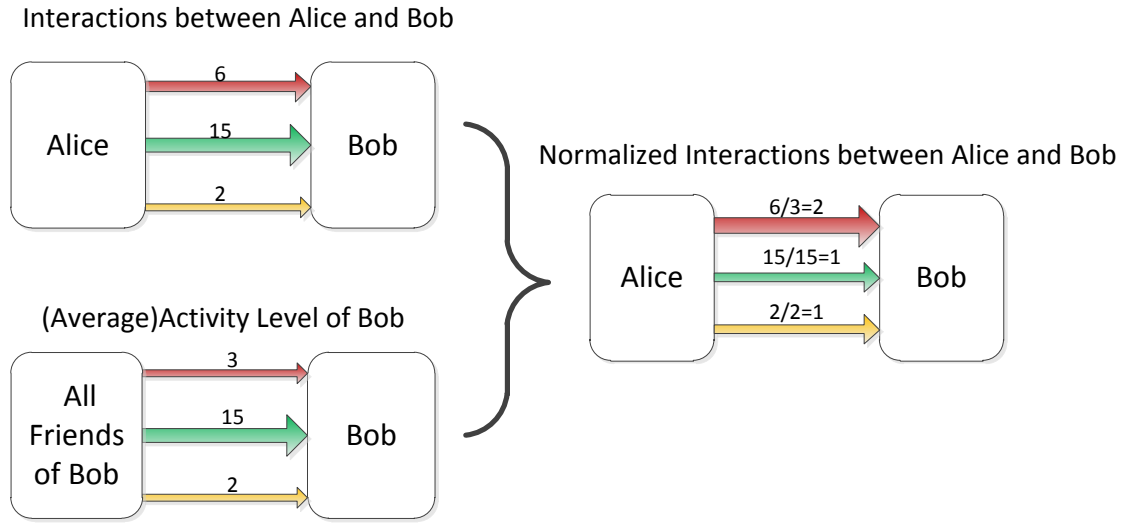


Figure 25. An example of data normalization

Finally, for each of the user's friend, we obtain an 'interaction vector' that includes twelve elements - normalized outgoing data for twelve types of interactions, which is, for any  $j \in F_i$ ,

$$\overrightarrow{s_{ij}} = \{\widetilde{s_{ij}^k}\}, k=1, 2, \dots, 12.$$

Based on those 'interaction vectors' (of all friends), an 'interaction matrix' could be constructed, which will be used by *itrust* to compute the user's friends' trustworthiness.

In the above example, the matrix will be:

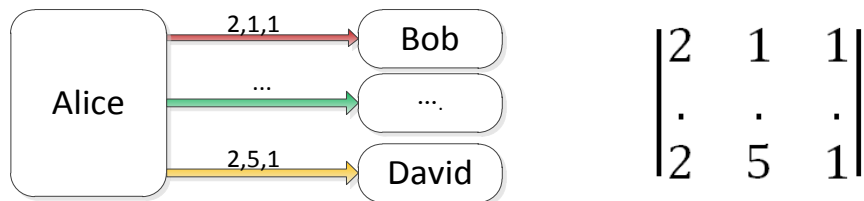


Figure 26.

### Trustworthiness Ranking

Two principles need to be stated before we compute interpersonal trust. First, the comparison of friends' trustworthiness is only valid from the perspective of a specific user. The reason is that different users perceive trust in different ways, and thus a user might be considered a close friend of one user, but an enemy of another. Second, trustworthiness is relative, so we only need to rank a user's friends based on their trustworthiness instead of computing the absolute trust values.

Although we have normalized interaction data, we cannot directly make use of them as correlations exist between different types of interactions. In other words, dependency and duplication in interactions must be removed. For example, 'tag photo' is the precondition of existing 'tag photo comments or likes', so the number of 'tag photo comments or likes' is highly depending on the number of 'tag photo'. To address this issue, we use the Principle Component Analysis (PCA) method, which not only removes correlation, but also objectively assigns weights/importance to different type of interactions.

PCA is a statistical procedure that uses orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of uncorrelated one. One objective of PCA is to find a small set of linear combinations of the variables (interaction data), so that the compounded variables (interaction data) are not correlated and thus avoid the multicollinearity problem. As shown in Figure 27, PCA is applied to extract the internal features from normalized 'interaction matrix'. For each feature, a



weight value will be generated and assigned. Those features are independent and represent a user's social interactions as well.

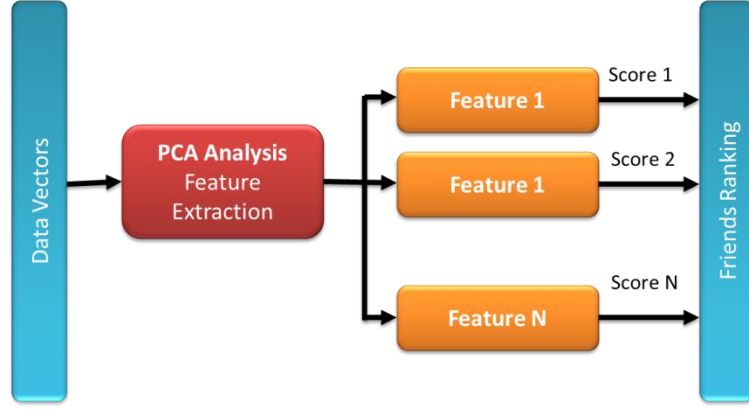


Figure 27. Flowchart of ranking generation

Extracted features are actually the combination of different types of interaction with different weights. Certainly, the features extracted from a user's 'interaction matrix' should be the same for all of her friends.

Details on PCA method applied on trust measurement in *itrust* are as follows:

Step 1: Interaction Matrix Establishment. For any  $j \in F_i$ , we have an interaction vector  $\vec{s}_{ij} = \{\widetilde{s}_{ij}^k\}$ ,  $k=1, 2, \dots, 12$ . Considering each  $\vec{s}_{ij}$  as a row in matrix, there would be  $|F_i|$  rows and 12 columns. That is to say, each column represents one type of interaction and each row represents the interactions between one friend  $j$  and the user  $i$ . We use  $X$  to denote the matrix.

Step 2: Interaction Matrix Standardization. As the range of different interactions varies, we need to smooth the data by converting each column to a mean of zero and a standard deviation of one.

$$Z_{ij}^k = \frac{\widetilde{s}_{ij}^k - \overline{x}^k}{v^k} \quad (6)$$

In which,

$$\overline{x}^k = \frac{\sum x^k}{|F_i|}, \quad v^k = \sqrt{\frac{\sum (s_{ij}^k - \overline{x}^k)^2}{|F_i| - 1}} \quad (7)$$

Step 3: Compute the Covariance Matrix,  $C = X^T X$ . The purpose is to find the relationships between 12 dimensional data sets. We calculate the eigenvectors of the covariance matrix and then select  $m$  eigenvectors that correspond to the largest  $m$  eigenvalues to be the new basis from  $u_1$  to  $u_m$ , and corresponding eigenvalues are from  $\lambda_1$  to  $\lambda_m$ .

Step 4: Calculate Score for Friend  $j$ :

$$S_j = \sum_{i=1}^m \frac{\lambda_i}{\sum \lambda_m} * u_i * Z_{ij} \quad (8)$$

By analyzing the features of all users in our dataset, we discover that six compounded interactions could represent 95% of the original ‘interaction vector’. Therefore, we use those six compounded interactions with corresponding weights to adjust the number of a user’s outgoing data towards each of his friends. Finally, a user’s friends are ranked based on the amount of her outgoing data transformed by PCA, i.e. the more outgoing data, the higher the trust levels.

## EVALUATION

In this chapter, we evaluate *itrust* by various trust evaluation tools. Based on the ground truth provided by users, we first examine the accuracy of *itrust* on head and tail of the ranking list (the correctness of ranking on most trustworthy and untrustworthy friends). Then, we test the accuracy of *itrust* based on Kendall's tau and generalized Kendall's tau, which are the predominate methods on ranking evaluation.

In each evaluation scenario, we compare the ranking result generated by *itrust* to the weighting [11] and regression methods [17]. Vedran [11] made a subjective evaluation on weight assignment for interaction factors, and their solution on weight assignment is shown in table 2.

Table 2. Weight assignment for each factor

Factors Weight	Weight Assigned
Co-tag	2
Status Comments	3
Status Likes	2
Inbox Messages	5
Photo Likes	1
Photo Comments	1

In the regression method, the model used is:

$$y = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_{12} x_{12} + \varepsilon \quad (9)$$

Where  $x_i$  denotes the number of interaction  $i$ , and  $y$  denotes the trust value.  $\varepsilon$  is the error variable. This model is used by Gilbert in [17] to predict social tie strength.

### Comparison to Ground Truth

After *itrust* finishes data collection and trustworthiness computation, a separated page is displayed to allow a user to evaluate the trustworthiness of her friends by dragging a sliding bar ranging from 0 to 100, as shown in Figure 28. We notice that users are often uncertain about how to translate subjective and multidimensional feelings about interpersonal trusts to a pre-labeled and linear scale. In addition, individual interpretations of interpersonal trust vary, so users are aware that accurate trustworthiness values are not required. However, the aggregated values consistently indicate the relative differences of interpersonal trust between her friends. Through this, we obtain the ground truth of a user's friends ranking based on their trustworthiness.

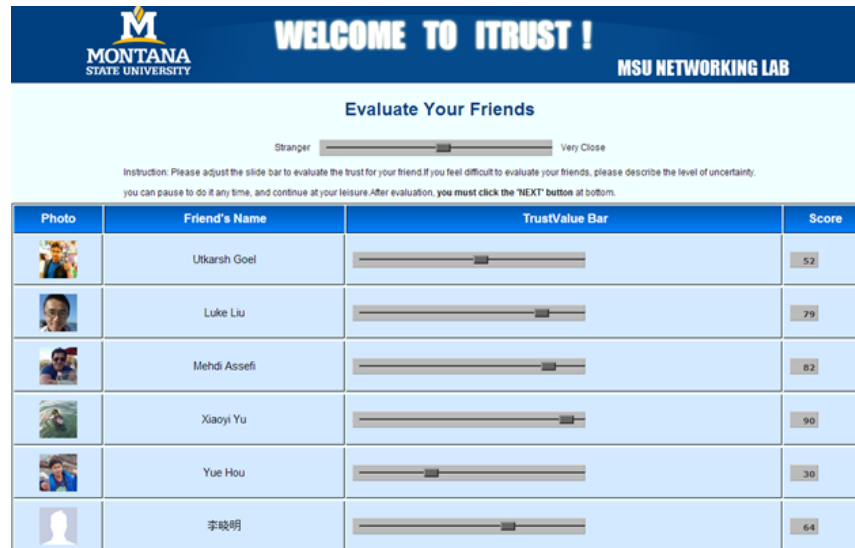







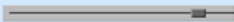

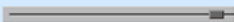

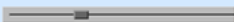

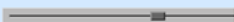
Photo	Friend's Name	TrustValue Bar	Score
	Utkarsh Goel		52
	Luke Liu		79
	Mehdi Assefi		82
	Xiaoyi Yu		90
	Yue Hou		30
	李晓明		64

Figure 28. Ranking evaluation interface

We select the user, whose friends cover the largest amount of users in the dataset, to evaluate the trust ranking generated by *itrust*. Figure 29 shows the differences between

the ranking generated by *itrust*, weighting and ground truth. Based on different ranking method, one element could be ranked in different positions. In the figure, the same element is connected by lines. So if most of these lines are horizontal or with small slopes, the ranking will be accurate. As shown in Figure 29, lots of skew lines exist between ground truth and ranking generated by weighting. Comparing to weighting method, the ranking list generated by *itrust* is more accurate.

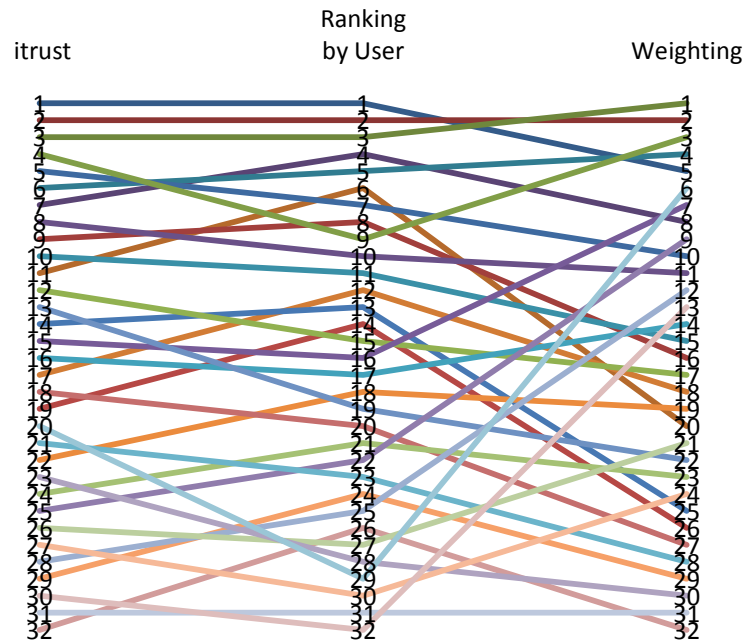


Figure 29. Ranking differences among *itrust*, weighting and ground truth

Figure 30 shows the differences between the ranking generated by *itrust*, regression and ground truth. Compared to the weighting method, there are fewer skew lines between ground truth and ranking generated by regression. However, we can still

see that lines between *itrust* ranking and ground truth are more horizontal, which indicates that *itrust* has a better performance on trust ranking.

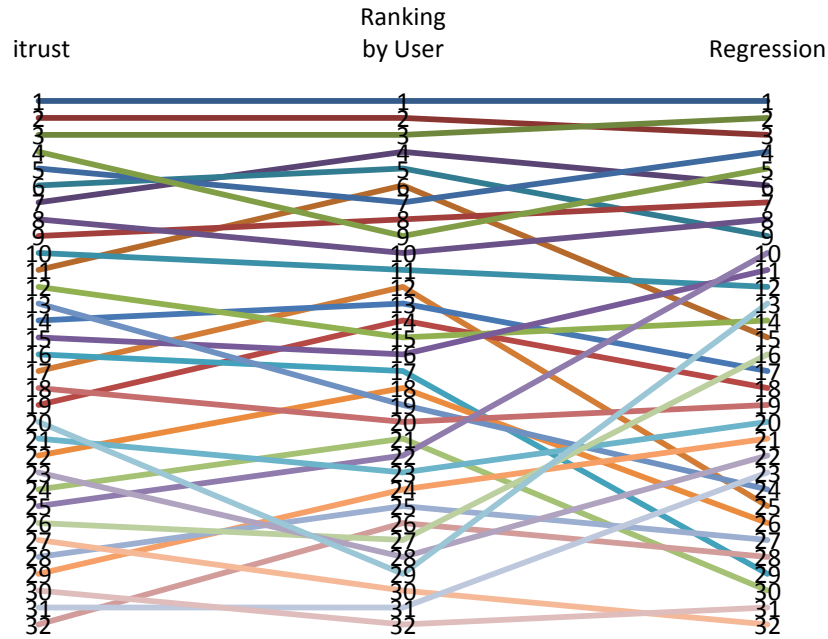
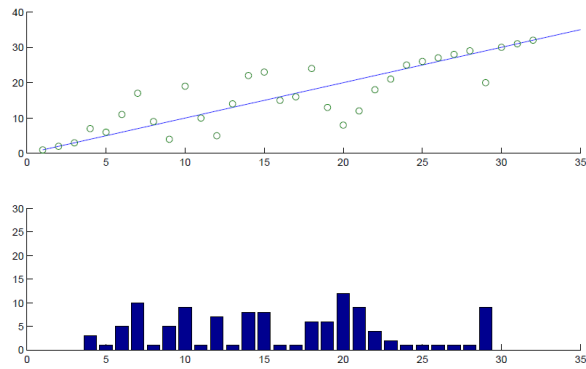
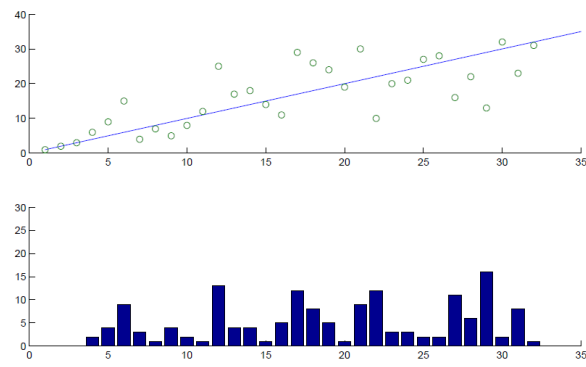
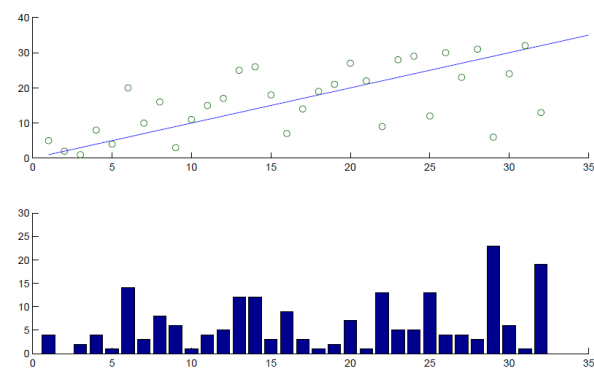


Figure 30. Ranking differences among *itrust*, regression and ground truth

Still analyzing the same user, the distributions of errors for each of her friends are described in Figure 31. For each ranking method, two sub figures are shown. In upper subfigures, the diagonal line is the ground truth, and circles represent the generated ranking. The closer distance between circles and the diagonal line, the more accuracy trust ranking is. Lower subfigures show the distribution of ranking differences for each of her friends. From these figures, we can conclude that the results generated by *itrust* are closer to the ground truth, compared to the regression and weighting methods.

(a) *itrust*

(b) Regression



(c) Weighting

Figure 31. Distribution of ranking result by *itrust*, regression and weighting

### Ranking Accuracy on Most Trustworthy and Untrustworthy Friends

The trustworthiness of friends on the head and tail of the ranking list are usually more important than those in the middle. This is because most applications tend to make use of trustworthy friends (e.g. to download files in P2P network) and avoid untrustworthy friends (to buy a product they recommended in e-commerce). Due to the above-mentioned reason, we first examine how accurate the trustworthiness is for those on the top and bottom 20% percentile of the ranking list.

$$S = \frac{x + y}{0.4|F|} \quad (10)$$

We use  $x$  (and  $y$ ) to denote the number of friends appearing on the top 20% (and bottom 20%) on the ranking list.  $|F|$  is the total number of the user's friends. Based on the above equation, ranking accuracies of different methods are shown in the Figure 32. The figure indicates that *itrust* provides more accurate ranking results on both top and bottom of the ranking list.

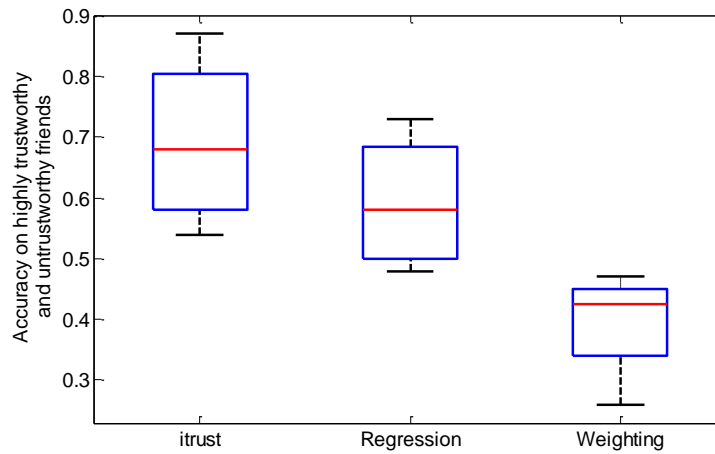


Figure 32. *itrust* accurately discovers highly trustworthy and highly untrustworthy friends



### Ranking Accuracy by Generalized Kendall's Tau

The above-mentioned method only considers trustworthiness accuracy of friends on the top and bottom percentiles of the ranking list, it is also necessary to evaluate the ranking accuracy for every friend on the list. To achieve this goal, we introduce the Kendall's tau method to quantify the difference of the ranking generated by users and that computed by *itrust*. Kendall's tau method is a well-recognized approach to compare two rankings. It uses the number of pair-wise disagreements to indicate the difference between two rankings. The smaller the difference, the more similar the rankings.

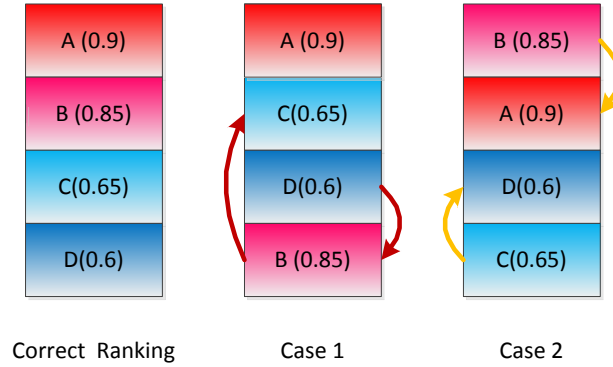


Figure 33. Illustrations of the Kendall's tau and generalized Kendall's tau methods

Figure 33 shows an example where the ground-truth ranking is 'ABCD', and two special cases are 'ACDB' and 'BADC', respectively. According to the Kendall's tau method, both case 1 and 2 have the same number of pair-wise disagreements, i.e. two disagreements (BC and BD) in case 1, and two (AB and CD) in case 2. Figure 34 shows the Kendall's tau coefficients between the ground-truth and the rankings generated by *itrust*, regression and weighting approaches, respectively. As shown in Figure 34, *itrust*

obtains the most accurate ranking results among these three methods, i.e. the average tau of *itrust* is 83%.

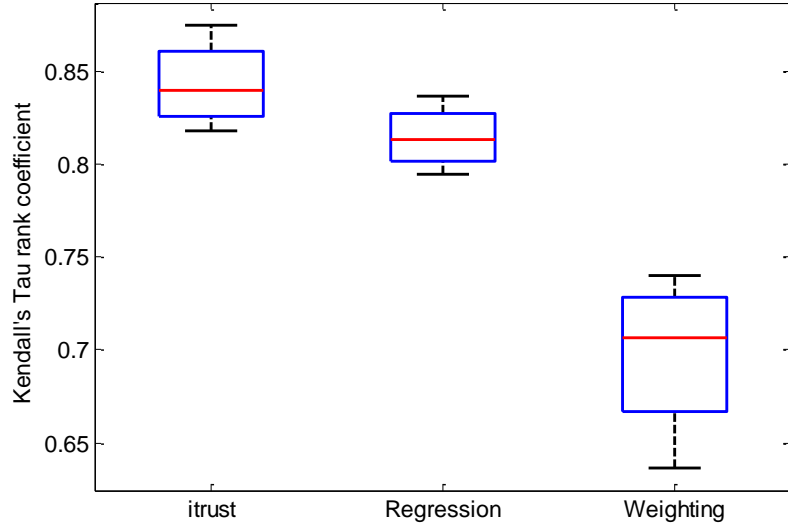


Figure 34. Evaluations based on Kendall's tau

Kendall's tau fails, however, to take into account the importance of different pair-wise disagreements, which is critical while evaluating the accuracy of a ranking list. To model the importance of each pair-wise disagreement, we adopt the Generalized Kendall's tau method. Generalized Kendall's tau (Gtau) considers elements weight, position weight, and trustworthiness similarities, while evaluate the difference between two rankings.

Unlike the Kendall's tau which counts the proportion of pair-wise agreements, Gtau computes the sum of weighted pair-wise disagreements. Therefore, the Kendall's tau method gives results ranging from 0 to 1 while Gtau returns results within various ranges, which highly depends on element and position weight, similarity values, and the

size of ranking list. In summary, the larger the results computed by Gtau (or the smaller the results generated by Kendall's tau), the more similar the two ranking lists are.

At a glance of Figure 33, the ranking error caused by swapping A and B should be bigger than that between B and C because most applications are only interested in trustworthy (or untrustworthy) information. Therefore, we add higher weights to elements on the top and bottom of a ranking list but lower weights to those in the middle. Moreover, ranking error caused by swapping B and D should be larger than that of C and D, because B and D are farther apart than C and D. Finally, the ranking error caused by swapping A and B should be bigger than that of B and C, because the trust values of A and B are more similar than B and C. In other words, both A and B are very close friends of the user but C is an acquaintance.

For each pair of disagreement  $(i, j)$  between two rankings, we assign the element and position weights based on the standard Normal Distribution, and assign the weight of trust similarities based on the trustworthiness values provided by user. We calculate the Gtau score by equation 11:

$$K = \sum_{i>j} w_i w_j \bar{p}_i \bar{p}_j D_{ij} [R_i < R_j] \quad (11)$$

where  $w_i$  is the element weight,  $p_i$  is the position weight and  $D_{ij}$  is the similarity difference between  $i$  and  $j$ .

For the element weight assignment, we divide the area under standard normal curve within  $(-3, 3)$  by the total number of elements  $n$ , and assign these proportions to the

elements. For the elements in head and tail of the list, bigger proportions (weights) are assigned. The element weight of  $i$  is calculated as follows:

$$w_i = 10 \int_{\frac{6(k-1)}{n}}^{\frac{6k}{n}} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \quad (12)$$

In which,  $n$  is the total number of elements in the ranking list, and  $k$  is defined as:

$$k = \left\lceil \frac{n+1}{2} - \left| i - \frac{n+1}{2} \right| \right\rceil$$

Figure 35 illustrates the element weight assignment visually. From the figure, we can see that elements in the head or tail of the ranking have larger weights, which means these elements are more important and the ranking errors on those elements are costly.

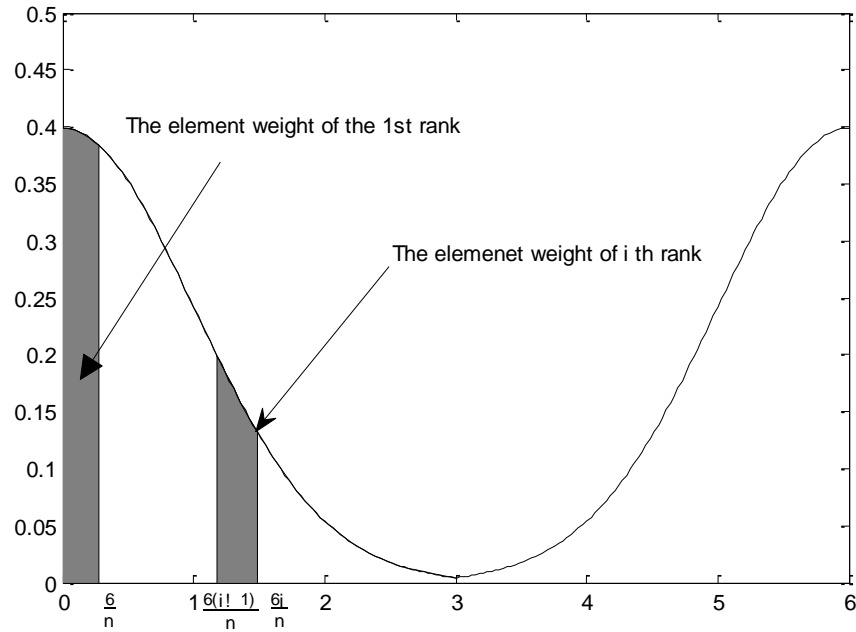


Figure 35. Illustration of element weight assignment

The position weight is defined as:

$$\bar{p}_i = \frac{p_i - p_{\delta(i)}}{i - \delta(i)} \quad (13)$$

In which

$$p_i = 10 \int_0^{\frac{6i}{n}} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \quad (14)$$

and  $\delta(i)$  is the position of element  $i$  in the second ranking list. The same as  $\bar{p}_i$ ,

$$\bar{p}_j = \frac{p_j - p_{\delta(j)}}{j - \delta(j)} \quad (15)$$

To put it simple, the further distance between two elements, the bigger position weight it will be assigned. At last, the similarity weight is defined as:

$$D_{ij} = (V_i - V_j)/100 \quad (16)$$

In which,  $V_i$  and  $V_j$  are the trust values of user  $i$  and  $j$ , respectively.

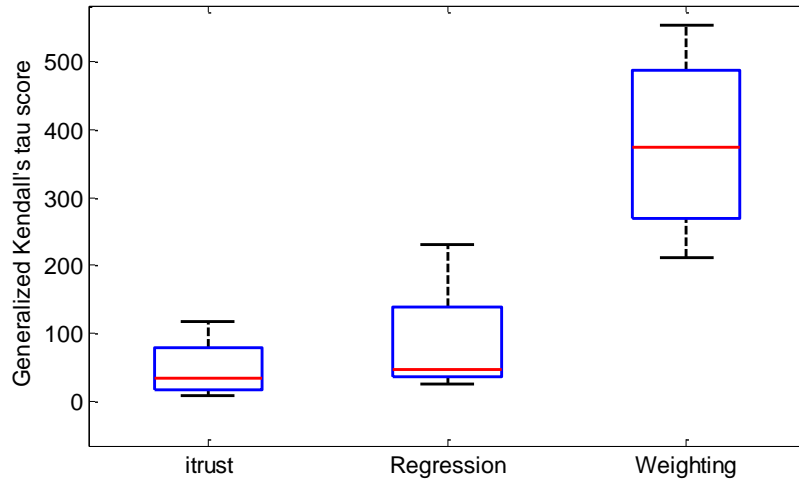


Figure 36. Evaluation based on Generalized Kendall's tau

By comparing the generated ranking and true friend ranking (ground truth provided by user), we calculate the Gtau score of each method and show the distribution of their Gtau scores are shown in Figure 36. Compared to the regression and weighting methods, the Gtau score of *itrust* has a smaller value range, which indicates that *itrust* offers much better ranking results compared to the other two methods.

## CONCLUSIONS

In this thesis, interpersonal trust relationships between Facebook users are measured by analyzing users' online social interactions. Since the amount of a user's online interaction data are highly influenced by the level of activity of her friends, the user's outgoing interaction data are first normalized by her friends' levels of activity. Then, with the PCA method, typical features of this user's interaction data are extracted and finally her friends' ranking list is generated. Evaluation results show that *itrust* provides more accurate trustworthiness ranking list than existing methods. Besides, *itrust* app is open to public and can be called from external application, which could be reused as a decision making mechanism. This work makes contributions to the understanding of interpersonal trust measurement in OSNs and provides promising results on inferring interpersonal trust from OSN. As to the future work, larger dataset with more Facebook users need to be collected to further evaluate the performance of *itrust*. Moreover, whether *itrust* is applicable to other types of OSN, e.g. Twitter or LinkedIn, is still need to be checked.

## REFERENCES CITED

1. Chiou, Shin-Yan, et al. "A trustable reputation scheme based on private relationships." *Social Network Analysis and Mining, 2009. ASONAM'09. International Conference on Advances in*. IEEE, 2009.
2. Li, Ze, and Haiying Shen. "Social-P2P: Social network-based P2P file sharing system." *Network Protocols (ICNP), 2012 20th IEEE International Conference on*. IEEE, 2012.
3. Kamvar, Sepandar D., Mario T. Schlosser, and Hector Garcia-Molina. "The eigentrust algorithm for reputation management in p2p networks." *Proceedings of the 12th international conference on World Wide Web*. ACM, 2003.
4. Zaczek, Lukasz, and Anwitaman Datta. "Mapping social networks into p2p directory service." *Social Informatics, 2009. SOCINFO'09. International Workshop on*. IEEE, 2009.
5. Popescu, Bogdan. "Safe and private data sharing with turtle: friends team-up and beat the system (transcript of discussion)." *Security Protocols*. Springer Berlin Heidelberg, 2006.
6. Pouwelse, Johan A., et al. "TRIBLER: a social-based peer-to-peer system." *Concurrency and Computation: Practice and Experience* 20.2 (2008): 127-138.
7. Lee, John D., and Katrina A. See. "Trust in automation: Designing for appropriate reliance." *Human Factors: The Journal of the Human Factors and Ergonomics Society* 46.1 (2004): 50-80.
8. Borum, Randy. "The science of interpersonal trust." (2010).
9. Huang, Dijiang, and Vetri Arasan. "On measuring email-based social network trust." *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010.
10. van den Bos, Wouter, Eric van Dijk, and Eveline A. Crone. "Learning whom to trust in repeated social interactions: a developmental perspective." *Group Processes & Intergroup Relations* 15.2 (2012): 243-256.
11. Podobnik, Vedran, et al. "How to calculate trust between social network users?." *Software, Telecommunications and Computer Networks (SoftCOM), 2012 20th International Conference on*. IEEE, 2012.
12. By the numbers: 105 Amazing Facebook Statistics.  
[http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/#.U2rYp\\_IdV8F](http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/#.U2rYp_IdV8F)
13. Massa, Paolo, and Paolo Avesani. "Controversial users demand local trust metrics: An experimental study on epinions. com community." *Proceedings of the National Conference on artificial Intelligence*. Vol. 20. No. 1. Menlo Park, CA; Cambridge, MA; London; AAAI Press; MIT Press; 1999, 2005.



14. Singh, Thomas B. "A social interactions perspective on trust and its determinants." *Journal of Trust Research* 2.2 (2012): 107-135.
15. Vishwanath, Arun. "Manifestations of interpersonal trust in online interaction A cross-cultural study comparing the differential utilization of seller ratings by eBay participants in Canada, France, and Germany." *New Media & Society* 6.2 (2004): 219-234.
16. Onnela, J-P., et al. "Structure and tie strengths in mobile communication networks." *Proceedings of the National Academy of Sciences* 104.18 (2007): 7332-7336.
17. Gilbert, Eric, and Karrie Karahalios. "Predicting tie strength with social media." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2009.
18. Nelson, R. B. "Kendall tau metric." *Encyclopaedia of Mathematics* 3 (2001): 226-227.
19. Kumar, Ravi, and Sergei Vassilvitskii. "Generalized distances between rankings." *Proceedings of the 19th international conference on World wide web*. ACM, 2010.
20. Jøsang, Audun, Roslan Ismail, and Colin Boyd. "A survey of trust and reputation systems for online service provision." *Decision support systems* 43.2 (2007): 618-644.
21. Ziegler, Cai-Nicolas. "On propagating interpersonal trust in social networks." *Computing with Social Trust*. Springer London, 2009. 133-168.
22. Quercia, Daniele, Stephen Hailes, and Licia Capra. "Lightweight distributed trust propagation." *Data Mining, 2007. ICDM 2007. Seventh IEEE International Conference on*. IEEE, 2007.
23. Golbeck, Jennifer, and James Hendler. "Inferring binary trust relationships in web-based social networks." *ACM Transactions on Internet Technology (TOIT)* 6.4 (2006): 497-529.
24. Overgoor, Jan, Ellery Wulczyn, and Christopher Potts. "Trust Propagation with Mixed-Effects Models." *ICWSM*. 2012.
25. Chen, Min, et al. "Method, system and server for managing friends' feed in network." U.S. Patent Application 13/611,180.
26. Jolliffe, Ian. *Principal component analysis*. John Wiley & Sons, Ltd, 2005.
27. Shakhnarovich, Gregory, and Baback Moghaddam. "Face recognition in subspaces." *Handbook of Face Recognition*. Springer London, 2011. 19-49.
28. López, Míriam, et al. "Principal component analysis-based techniques and supervised classification schemes for the early detection of Alzheimer's disease." *Neurocomputing* 74.8 (2011): 1260-1271.
29. Price, Alkes L., et al. "New approaches to population stratification in genome-wide association studies." *Nature Reviews Genetics* 11.7 (2010): 459-463.

30. Steiner, João E. "World university rankings-A principal component analysis." *arXiv preprint physics/0605252* (2006).
31. Xiaofeng Gao. Construction of Evaluation System of Faculty Resource in Major Universities by using Principal Components Analysis(2003).
32. Sharma, Soumitra. "Principal component analysis (PCA) to rank countries on their readiness for e-tail." *Journal of Retail & Leisure Property* 7.2 (2008): 87-94.
33. Manage, Ananda BW, and Stephen M. Scariano. "An Introductory Application of Principal Components to Cricket Data." *Journal of Statistics Education* 21.3 (2013). Ranking definition.

## APPENDICE

APPENDIX A: User Consent on Using itrust

Title: Understanding Interpersonal Trust based on Social Network User Interactions

“ You are being asked to participate in a research study of understanding interpersonal trust based on social network user interactions. People tend to interact intensely with a small subset of friends, carrying out a social grooming in order to maintain and nurture strong and trustful ties. This study will help us obtain a better understanding of how interactions between online social network users can reflect the interpersonal trust between them.

You have been identified as a possible subject because you have at least 2-month experience in using Facebook, or one of your Facebook friends recommends you. If you agree to participate, you will be asked to login to your Facebook account and go to the *itrust* app. The whole experiment should be finished within 2 minutes. Participation is voluntary!

After logging into Facebook.com and clicking the *itrust* app, you need to wait less than 2 minutes to allow the *itrust* app to collect your interaction data. The time *itrust* takes to collect data depends on how frequently you interacted with your friends, and how many friends you have. Interaction data being collected include the numbers of inbox messages, photo comments, photo likes, album comments, album likes, tags, tagged, tag-photo comments, tag-photo likes, co-tags, status likes, and status comments. Data collected in this experiment is retrieved for aggregated evaluation, and original

data/text will not be stored anywhere. User names will be coded, so it is impossible to track an user's ID based the stored data. An example of data entry stored on the MSU server looks like:

name	friendname	inbox	pcomments	plikes	acomment	alikes	tag	tagged	tpcomments	tplikes	cotags	scomments	slikes
a12d	a1646843	0	3	1	0	2	1	2	1	2	0	0	3

Data collected in this experiment will be kept confidential on MSU servers with access restricted to investigators. Data collected in the experiment will be aggregated and made public without links to your personal information. Risks involved in this study include fatigue and eye strain. If you experience such problems, please quit the experiment immediately. After the completion of the survey you will automatically be entered into a drawing for fabulous prizes!

Grand prize \$100.00 Visa Gift Card Total Winner: 1

Second prize \$50.00 Visa Gift Card Total Winners: 2

Third prize \$25.00 Visa Gift Card Total Winners: 4

There is no cost on your part for participation. There will be no consequences if you decline to participate. If you have questions about the research you can contact Qing Yang at 406-994-3547.[qing.yang@cs.montana.edu]. If you have additional questions about the rights of human subjects, you can contact the Chair of the Institutional Review Board, Mark Quinn, (406) 994-4707 [mquinn@montana.edu].