To Trust or Not to Trust? Predicting Online Trusts using Trust Antecedent Framework

Viet-An Nguyen, Ee-Peng Lim, Jing Jiang
School of Information Systems
Singapore Management University, Singapore
{*vanguyen,eplim,jingjiang*}@*smu.edu.sg*

Aixin Sun
School of Computer Engineering
Nanyang Technological University, Singapore
axsun@ntu.edu.sg

***Abstract*—This paper analyzes the trustor and trustee factors that lead to inter-personal trust using a well studied Trust Antecedent framework in management science [10]. To apply these factors to trust ranking problem in online rating systems, we derive features that correspond to each factor and develop different trust ranking models. The advantage of this approach is that features relevant to trust can be systematically derived so as to achieve good prediction accuracy. Through a series of experiments on real data from Epinions, we show that even a simple model using the derived features yields good accuracy and outperforms MoleTrust, a trust propagation based model. SVM classifiers using these features also show improvements.**

***Keywords*-Trust prediction, trust ranking, trust antecedent framework.**

I. Introduction

A. Motivation

In this paper, we study how trusts can be directly inferred from rating data. Our research works on the premise that user rating behaviors reflect the trusts among users. For example, users are likely to give higher ratings to people they trust than others. Users are likely to be more interested consuming objects contributed by people they trust.

In organizational behavior research, there is a well established **Trust Antecedent (TA) framework** which derives **ability**, **benevolence** and **integrity** as the three key factors of a trustee that leads to trust conferred on him or her[10]. This framework, shown in Figure 1, essentially says that a trustee is given trust if s/he is perceived to have skills and competence to deliver desired outcome (*ability*), to want to do good with the trustor (*benevolence*), and to adhere to a set of good moral principles (*integrity*). Moreover, the willingness of a trustor to trust others, known as **trust propensity** is another factor of trustor that determines how easy a trustor trusts someone. Hence, we have a total of three main *trustee factors* and one main *trustor factor* that facilitate trust between a trustor and a trustee. Once a trust is formed with a trustee, the trustor is more willing to take more risk. The outcome of risk taking will serve as feedback to modify the perception about trustee's ability, benevolence and integrity. TA framework has been widely validated on users in both the organization and e-commerce settings [6], [2].

This work is partially supported by Singapore's National Research Foundation's research grant, NRF2008IDM-IDM004-036.

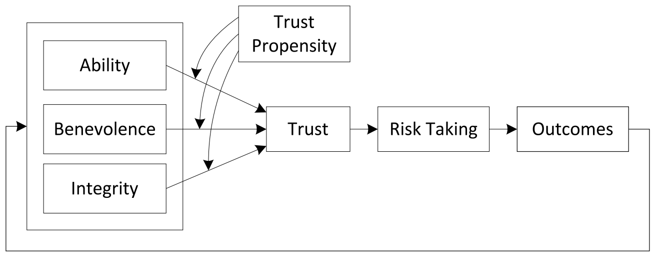

Figure 1. Trust Antecedent Framework

Although the TA framework has been widely adopted by researchers in management science, it has not been investigated for developing *quantitative* trust models for online communities. In quantitative trust models, we aim to compute numerical weights for trusts between users indicating the extent to which trusts are built among them. This is essential as quantitative trust models can be more readily integrated with applications, e.g. search and recommendation.

B. Research Objectives

In this research, we focus on studying quantitative trust models for online rating systems based on the TA framework. This requires the qualitative factors in the framework to be mapped into some measurable feature values that can be used to build quantitative trust models. Our purpose is to use these trust models to infer or predict trusts among users using rating data and the very sparse trust data. Each trust model assigns for each given user pair a trust score in the range of [0,1] with 0 representing *complete no-trust* and 1 representing *complete trust*. Once trust scores are assigned, we can rank the trust relationships of all user pairs by trust score and evaluate the prediction accuracy of the different proposed trust models.

Two main research contributions of this paper are summarized as follows:

- The ability, benevolence, integrity and trust propensity factors of trust antecedent framework are carefully analyzed before we propose a range of different quantitative trust models that are based on measurable features derived from these factors. To the best of our knowledge, this is the first attempt developing quantitative trust models from a qualitative one.
- Our proposed quantitative trust models are evaluated using a large Epinions dataset that provides the WOT ground truth data. We show that our proposed trust models outperform MoleTrust which is based on trust propagation [8] and some of them are close to SVM-based trust prediction model despite not using any sophisticated training.

C. Paper Organization

The remainder of the paper is organized as follows. We survey the related work in Section II. The trust ranking problem and the Epinions dataset used in our work are introduced in Section III. We then propose our trust ranking models in Section IV and evaluate them in Section V. We finally conclude the paper in Section VI.

II. Related Work

Independent to the TA framework developed in management science, the computer science research community has focused on three main types of trust models, namely *trust evaluation*, *trust prediction* and *trust propagation*. Trust evaluation refers to developing the trust scoring system of some P2P or Web application so as to derive a global trust score to each node or user in the user community[11], [5].

In trust prediction, classification methods are developed to assign trust class labels and weights to candidate user pairs. Liu et.al developed a taxonomy of user and interaction features to represent a user pair and a SVM-based method to classify candidate user pairs [7]. Matsuo and Yamamoto proposed another SVM-based method to assign trust class labels using features extracted from user profiles, product reviews and trust relations[9]. The above works however developed their feature sets based on data centric grouping instead of trust factors. Hence, one may miss out features that belong to some trust antecedent(s) and subsequently construct less optimal trust models.

Trust propagation represents a body of trust model research that focuses on using trust propagation to infer new trust relationships between users [3], [8], [1]. For example, if user u_i trusts u_j and u_j trusts u_k, one may infer that u_i trusts u_k. As the name suggests, trust models based on trust propagation are very much dependent on trust connectivity among users. They may not work well when such connectivity is sparse.

III. Preliminaries

A. Trust Ranking Problem

Let $\mathbf{U} = \{u_1, u_2, \cdots, u_n\}$ represent a set of unique users whose rating information and trust relationships are recorded from time points 1 to Z. At some time point $z \in [1, Z]$, we say that a *trustor-trustee pair* (or *trust pair* for simplicity) (u_i, u_j) is formed when user u_i creates a trust relationship to user u_j. It is possible that a trust pair is removed after some time but this is rare and we have decided not to consider trust pair removal in this research.

Let $\mathbf{R} = \{r_1, r_2, \cdots, r_m\}$ denote the set of reviews written by users in $\mathbf{U}$. The user who wrote a review r_k is denoted by $w(r_k)$. The rating score that a user u_i gives to review r_k is denoted by s_{ik}. We use $\mathbf{R}_{ij}$ to denote the set of reviews written by user u_j and rated by user u_i; $\mathbf{U}_k^{\mathcal{R}}$ to denote the set of users who rate the review r_k. If user u_i rates a review written by user u_j, (u_i, u_j) is called a *review rater-writer pair* (or *rating pair* for simplicity).

We would like to address trust prediction in online rating systems as a **trust ranking problem**. Given a set of candidate trustor-trustee pairs, a trust ranking method will assign a *trust score* to each pair. Candidate pairs can then be sorted in descending score values and highly ranked pairs are considered more likely to form trust relationships.

Formally, the trust ranking problem can be defined as follows: *Given a set of rater-writer pairs* $\mathbf{G}$*, the corresponding review rating information* $\bigcup_{(u_i,u_j)\in\mathbf{G}}(\{s_{ik} \mid r_k \in \mathbf{R}_{ij}\} \cup \{s_{jk} \mid r_k \in \mathbf{R}_{ji}\})$ *(i.e., ratings between users of rating pairs* (u_i, u_j)*'s in* $\mathbf{G}$*) and known trustor-trustee pairs* $\mathbf{T}$*, find the ranks of* (u_i, u_j) *pairs using their trust score values* t_{ij}*'s.*

B. Overview of Proposed Solution Framework

Given that the trust antecedent (TA) framework has three factors about a trustee (i.e., *ability*, *benevolence* and *integrity*) and one factor (trust propensity) about a trustor as antecedents of trust, we would like to derive for each of them a set of relevant features. This eventually leads us to a meaningful set of features for representing a candidate trust pair.

The ability, benevolence and integrity factors are perceived knowledge about trustees [10]. In other words, a person A who is perceived to have good ability by person B may be perceived to have poor ability by person C. The same applies to benevolence and integrity. This suggests that *ability, benevolence and integrity are specific to the trustor and candidate trustee* even though they are properties of the candidate trustee. This observation has major implications to the way we derive features for representing the three factors. We therefore would need the ability, benevolence and integrity features to be derived from interactions the trustor have with the candidate trustee.

Trust propensity, on the other hand, is a factor that is associated with the trustor and it does not depend on

Table I
STATISTICS OF DATASET

Description	Number
$\|\mathbf{U}\|$ = # users	131,828
$\|\mathbf{T}_0\|$ = # trust pairs for $z = 0$	506,934
$\|\mathbf{T}_{[1,Z]}\|$ = # trust pairs for $z \in [1, 499]$	151,230
$\|\mathbf{R}\|$ = # reviews	1,198,115
$\|\mathbf{G}_0\|$ = # rating pairs for $z = 0$	3,024,664
$\|\mathbf{G}_{[1,Z]}\|$ = # rating pairs for $z \in [1, 499]$	1,468,322

candidate trustee at all. Hence, *trust propensity is a global trustor property* that can be measured by features derived from all interactions a trustor have with all users. We will elaborate on the features derived from rating interaction data for the four factors in Section IV.

C. Extended Epinions Dataset

An extended Epinions dataset has been obtained from the Trustlet website[1] as the rating and trust data for our experiments. The same dataset has been used in [3], [8]. In Epinions, a (dis)trust relationship is directional from the *(dis)trustor* to the *(dis)trustee*. The trust relationships of a user's WOT are publicly available to all other users while the distrust relationships can only be seen by the user. The dataset contains all product reviews and reviews ratings (*review rating data*) as well as the Web of trust and distrust relationships (*trust/distrust data*) obtained on 10 January 2001. These data do not carry any timestamps but are artificially assigned timestamp $z = 0$ to distinguish them from other data. The dataset also provides the daily review rating data from 17 January 2001 to 30 May 2002 (i.e., 499 days) and the daily trust/distrust data from 17 January 2001 to 12 August 2003 (938 days). In this paper, rating and trust data from 17 January 2001 to 30 May 2002 are used and are assigned timestamps $z = 1$ to 499 respectively. Our experiments exclude trust data from 31 May 2002 to 12 August 2003. The statistics of the dataset used in our experiments is given in Table I.

IV. PROPOSED MODELS FOR TRUST RANKING

In this section, we will describe eight trust ranking models by combining different trust antecedent factors. Each factor can be quantitatively measured by one or more features derived from the interaction data between users and each model is simply a product of these features.

A. Ability-Only ($\mathcal{A}$) Models

An Ability-Only Model defines trust likelihood score of a candidate trustor-trustee pair (u_i, u_j) based on the ability of candidate trustee perceived by the trustor. In Epinions, u_i has several ways to perceive the ability of u_j, some more direct and others more subtle. We propose the following two features that may more directly depict the candidate trustee's (or u_j's) ability, and call them the **ability features**:

- **Average rating u_j received from u_i ($\overline{s_{ij}}$)**: This refers to the average of all u_i's ratings on reviews by u_j. We expect this average rating tells how good u_i thinks of reviews written by u_j. To keep the average rating within [0,1], we convert the raw rating scores to [0,1] by mapping 1 to 5 stars to 0.2, 0.4, 0.6, 0.8 and 1.0 respectively. Formally, $\overline{s_{ij}}$ is defined as:

$$\overline{s_{ij}} = \frac{1}{|\mathbf{R}_{ij}|} \sum_{r_k \in \mathbf{R}_{ij}} s_{ik} \tag{1}$$

- **Interaction intensity from u_i to u_j (i_{ij})**: This refers to the number of reviews of u_j rated by u_i. This is equivalent to the number of ratings u_i give to u_j's reviews. Unlike average rating $\overline{s_{ij}}$ which does not consider that most users only rate very few reviews, interaction intensity i_{ij} counts the number of u_j's reviews rated by u_i as the perceived ability of u_j.
To examine more closely the relationship between the number of ratings and trust relationship, we analyzed the aggregated rating data between trust and non-trust rating pairs. Figure 2 depicts the long-tailed distributions of the rating count for trust and non-trust pairs. Note that the bin sizes are different for different ranges of rating count. Among the rating pairs having small rating count (< 10), non-trust pairs dominate 92.54% of the pairs. However, the proportions of trust pairs and non-trust pairs become more balanced (45.93% and 54.07% respectively) among the set of pairs having rating count $\geq$ 10. When rating count $\geq$ 100, it is obvious that trust pairs dominate.

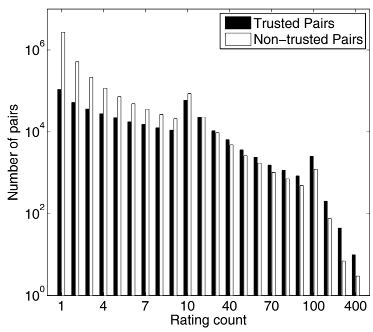

Figure 2. Distribution of Number of Ratings

Given that the number of rated reviews can vary from 1 to a very large number, we derive the normalized version of i_{ij} by applying a transformation function $\mathfrak{F}$ as follows:

$$i_{ij} = \mathfrak{F}(|\mathbf{R}_{ij}|, \alpha, \mu) \tag{2}$$

[1] http://www.trustlet.org/wiki/Extended_Epinions_dataset

where

$$\mathfrak{F}(x, \alpha, \mu) = \frac{1}{1 + e^{-\alpha(x-\mu)}} \tag{3}$$

In Equation 3, the sigmoid function in $\mathfrak{F}$ was chosen to keep the returned value in the range of $[0, 1]$ as well as to reduce the effect of the large x. α ($\in \mathbb{R}^+$) and μ ($\in \mathbb{Z}^+$) decide the slope and controls the midpoint of the sigmoid curve respectively. More specifically, $\mathfrak{F}$ is close to 0 when x is small, equal to 0.5 if $x = \mu$ and asymptotically to 1 when x gets very large. In our experiments, we use $\mu = 5$ so as to assign i_{ij} of > 0.5 to minority of user pairs with more rating interaction as $|\mathbf{R}_{ij}|$ largely follows a power law distribution. We use $\alpha = 0.1$ although several other α values are found to work quite well too.

Given that we have the above two ability features, we now define three ability-only models as follows:

- $\mathcal{A}(\mathcal{AR})$ **Model**: For this model, we only use the average rating from u_i to u_j for scoring trust from u_i to u_j. That is:
$$t_{ij} = \overline{s_{ij}} \tag{4}$$
- $\mathcal{A}(\mathcal{I}^2)$ **Model**: This model uses the interaction intensity for scoring trust.
$$t_{ij} = i_{ij} \tag{5}$$
- $\mathcal{A}(\mathcal{AR} + \mathcal{I}^2)$ **Model**: This model combines the two ability features to score trust from u_i to u_j.
$$t_{ij} = \overline{s_{ij}} \cdot i_{ij} \tag{6}$$

B. Benevolence-Only ($\mathcal{B}$) Model

Benevolence is often associated with characteristics such as helpfulness, caring, loyalty, receptivity, etc.. In the online rating setting, there is no direct feature that can be used for measuring benevolence. We however know that different users have different standards in giving ratings. The *stringent* users give lower ratings while the *lenient* ones give higher ratings. For a given user u_i, such leniency characteristics can be *global* if we consider all ratings u_i gives, or *local* if only ratings u_i gives to the reviews of another user u_j are considered. In the following, we derive a local version of leniency l_{ij}.

Local leniency from user u_i to u_j (l_{ij}). We propose to measure the local leniency l_{ij} by the relative difference between the u_i ratings on the reviews written by u_j and the actual quality of these reviews. Let $\mathbf{R}_{ij}$ denote the set of reviews written by u_j and rated by u_i, and q_k ($\in$ [0,1]) represents the quality of a review r_k in $\mathbf{R}_{ij}$. We then define l_{ij} as:

$$l_{ij} = \underset{r_k \in \mathbf{R}_{ij}}{\text{Avg}} \left(\frac{s_{ik} - q_k}{s_{ik}} \right) \tag{7}$$

Equation 7 produces a leniency value in $(-\infty, +\infty)$. The zero, positive and negative leniency values indicate a user is neutral, lenient and stringent respectively. The equation also requires the *quality* of each review r_k to be known. One can take the average of s_{*k}'s (i.e., all ratings on r_k) as q_k but this approach does not consider that s_{*k}'s are also affected by user leniency l_{ij}'s. One should adjust $s_{i'k}$ score lower if $u_{i'}$ is lenient and higher if $u_{i'}$ is stringent. Furthermore, a review r_k with too few ratings are not likely to have good q_k. In the following, we therefore define q_k as an average of s_{*k}'s adjusted by user leniency multiplied by *popularity score* (denoted by o_k) of review r_k as follows.

$$q_k = o_k \cdot \underset{u_i \in \mathbf{U}_k^{\mathcal{R}}}{\text{Avg}} \left(s_{ik} \cdot (1 - \beta \cdot l_{i\ w(r_k)}) \right) \tag{8}$$

where

$$o_k = \mathfrak{F}(|\mathbf{U}_k^{\mathcal{R}}|, \alpha', \mu') \tag{9}$$

β is a value in [0,1] to control the maximum amount of score adjustment on s_{ik}. Intuitive, β should not be near 1. In our experiments, we set β to 0.5. Other β values ($<$ 0.8) have been experimented and they gave almost the same results. Similar to normalization of i_{ij} in Equation 2, o_k is normalized using the $\mathfrak{F}$ function with α' and μ' parameters. In our experiments, we set α' and μ' to be 0.1 and 5 respectively for reasons similar to those of Equation 2.

Equation 9 can be easily computed. Leniency and quality values in Equations 7 and 8 can be solved by iterative computation which first assigns l_{ij} to be 0 in computing q_k's. This is followed by computing a new set of l_{ij} values which are in turn used in computing a new set of q_k's. This process repeats until some convergence is reached.

We now define the **benevolence feature** b_{ji} from candidate trustee u_j to trustor u_i as benevolence-only model as a mapping of l_{ji} to the range of [0,1]:

$$b_{ji} = \frac{l_{ji} - \text{Min}_{\ u'_j\ u'_i}\, l_{j'i'}}{\text{Max}_{\ u'_j\ u'_i}\, l_{j'i} - \text{Min}_{\ u'_j\ u'_i}\, l_{j'i}} \tag{10}$$

We then define our **Benevolence-Only ($\mathcal{B}$) Model** as:

$$t_{ij} = b_{ji} \tag{11}$$

C. Integrity-Only ($\mathcal{I}$) Model

Integrity is related to a person's commitment to his or her promises to others. Similar to benevolence, there is no direct feature from online rating data that measures a candidate trustee's integrity perceived by a trustor. Instead of leaving out this factor completely, we have introduced a feature to measure the global trustworthiness of the candidate trustee u_j by number of other users who trust him/her. Hence, the **integrity feature** of u_j is the mapping of trustworthiness to the range of [0,1]:

$$x_j = \mathfrak{F}(|\mathbf{U}_{*j}^{\mathcal{T}}|, \alpha'', \mu'') \tag{12}$$

Again, the parameters α'' and μ'' are set to 0.1 and 5 respectively following the same arguments for Equations 2 and 9.

The **Integrity-Only ($\mathcal{I}$) Model** is then defined by:

$$t_{ij} = x_j \tag{13}$$

Since this model depends on x_j only, it is not able to distinguish different trustors for the same candidate trustee.

D. Ability, Benevolence and Integrity ($\mathcal{ABI}$) Model

We can combine the different ability, benevolence and integrity features together to arrive at different trust models. In this paper, we will focus on the $\mathcal{A}(\mathcal{AR}+\mathcal{I}^2)\mathcal{BI}$ Model that involves all the three key trust factors. As will be shown in Section V, $\mathcal{A}(\mathcal{AR}+\mathcal{I}^2)\mathcal{BI}$ model outperforms both $\mathcal{A}(\mathcal{AR})$ and $\mathcal{A}(\mathcal{I}^2)$ models. The $\mathcal{AR}+\mathcal{I}^2$ features are therefore used in the **Ability, Benevolence and Integrity** ($\mathcal{ABI}$) **Model**.

$$t_{ij} = i_{ij} \cdot \overline{s_{ij}} \cdot b_{ji} \cdot x_j \tag{14}$$

E. ABI with Trust Propensity ($\mathcal{ABIT}$) Model

We introduce the following two **trust propensity features**, the first based on global leniency a trustor u_i shows to his or her trustees and the second based on the number of trustees u_i has:

- **Global Leniency of** u_i (p_i):

$$p_i = \underset{j}{\text{Avg}} \; \frac{l_{ij} - \text{Min}_{\;u_i'\;u_j'}\, l_{i'j'}}{\text{Max}_{\;u_i'\;u_j'}\, l_{i'j'} - \text{Min}_{\;u_i'\;u_j'}\, l_{i'j'}} \tag{15}$$

- **Normalized Trust Outdegree of** u_i:

$$y_i = \mathfrak{F}(|\mathbf{U}^{\mathcal{T}}_{i*}|, \alpha^{\#}, \mu^{\#}) \tag{16}$$

Given a trustor u_i, we use $\mathbf{U}^{\mathcal{T}}_{i*}$ to denote the set of users that u_i trusts. The parameters $\alpha^{\#}$ and $\mu^{\#}$ are set to 0.1 and 5 respectively following the same arguments for Equations 3, 9 and 12.

Two $\mathcal{ABI}$ with Trust Propensity ($\mathcal{ABIT}$) Models are then defined by:

- $\mathcal{ABIT}(\mathcal{L})$ **Model**:

$$t_{ij} = i_{ij} \cdot \overline{s_{ij}} \cdot b_{ji} \cdot x_j \cdot p_i \tag{17}$$

- $\mathcal{ABIT}(\mathcal{T})$ **Model**:

$$t_{ij} = i_{ij} \cdot \overline{s_{ij}} \cdot b_{ji} \cdot x_j \cdot y_i \tag{18}$$

V. Experiments and Results

Experiment design. We first conduct experiments to evaluate the performance of the eight proposed trust models ($\mathcal{A}(\mathcal{AR})$, $\mathcal{A}(\mathcal{I}^2)$, $\mathcal{A}(\mathcal{AR}+\mathcal{I}^2)$, $\mathcal{B}$, $\mathcal{I}$, $\mathcal{ABI}$, $\mathcal{ABIT}(\mathcal{L})$, and $\mathcal{ABIT}(\mathcal{T})$ Models) on the whole dataset (data with $z = 0$ and 1 to 499). We also compare our models with MoleTrust with and without propagation path length constraint[8] (see Section II). The first MoleTrust model, denoted by *MoleTrust0*, does not impose any path length constraint for trust propagation. The second MoleTrust model, denoted by *MoleTrust2*, imposes a path length constraint of 2. Both *MoleTrust0* and *MoleTrust2* use the same trust score threshold of 0.6 which was also used in the earlier work [8]. Both MoleTrust models use trust and distrust edges assigned with weights of 1 and 0 respectively.

To evaluate the different models, we randomly chose 1000 trust pairs and the other 1000 non-trust pairs and performed trust ranking on them using all the models. All the candidate pairs have to satisfy the following conditions:

- There exists some review write-rate interaction(s) between the trustor and trustee candidates in the dataset (i.e., from time point 0 to Z). This is to allow the models to score the candidate pairs from rating data.
- There exists some directed path in the graph of trust and distrust relationships from the trustor to trustee for each trust pair to be scored. This is to give MoleTrust some path for trust propagation for scoring the trust pair.

We carried out experiments on 5 different samples of trust and non-trust pairs and all the experimental results shown below are averaged over the 5 runs. In this experiment, we also applied SVM^{light} [4] with linear kernel using the 8 trust features shown in Table II. To compare with the results of earlier work, we show the results of SVM using 13 most important features[2] identified by [7] and the results using these 13 features and our 8 features. We denote the two results by **SVM13** and **SVM21** respectively.

Performance metrics. We measured the ranking accuracy by $F1$. We ranked the candidate pairs using each trust model and predicted the top scored 1000 pairs as trust pairs. The precision, recall and $F1$ measured from these predicted results are identical and is defined as $\frac{Num.\ of\ correctly\ predicted\ trust\ pairs}{1000}$. Since there are equal numbers of trust and non-trust pairs, the $F1$ of random selection of 1000 trust pairs is 0.5. We therefore expect the $F1$ of a good model to be $>$ 0.5. For MoleTrust0 and MoleTrust2, we observed for each run that only a subset of 2000 candidate pairs that assign trust scores. Let M be the number of trust pairs with some trust scores produced by a MoleTrust model. $F1$ is thus defined as $\frac{Num.\ of\ correctly\ predicted\ trust\ pairs\ at\ top\ M}{M}$ giving some advantage to MoleTrust0 and MoleTrust2 over the other models. In the case of SVM, we used 5-fold cross validation on each run of data with stratified numbers of trust and non-trust pairs. For each of the 5 rounds of evaluation, four subsets were used as training data and the remaining one subset was used as test data. The mean $F1$ is then obtained from the $F1$'s obtained for 5 rounds of test data. We then averaged the mean F1 values over the 5 runs.

Results. The second column of Table III[3] shows the $F1$ results of the eight proposed trust models and two MoleTrust

[2] Some important features were excluded due to their non-existence in our Epinions dataset.

[3] The best F1 value in each group is boldfaced.

Table II
FEATURE WEIGHTS GENERATED BY SVM

Feature	Weight (Trustor Indep. Evaluation)
$\overline{s_{ij}}$	0.172
i_{ij}	0.263
$\overline{s_{ij}} \cdot i_{ij}$	0.194
$\overline{q_k}$	0.064
b_{ji}	**0.776**
x_j	0.004
p_i	0.027
y_i	-0.092

Table III
F1 RESULTS

Models	F1 of Trust Indep. Evaluation
MoleTrust-0	0.513
MoleTrust-2	**0.540**
$\mathcal{A}(\mathcal{AR})$	0.577
$\mathcal{A}(\mathcal{I}^2)$	0.710
$\mathcal{A}(\mathcal{AR}+\mathcal{I}^2)$	0.725
$\mathcal{B}$	0.733
$\mathcal{I}$	0.648
$\mathcal{ABI}$	0.734
$\mathcal{ABIT}(\mathcal{T})$	0.692
$\mathcal{ABIT}(\mathcal{L})$	**0.745**
SVM	**0.771**
SVM13	0.739
SVM21	**0.780**

models. MoleTrust0 and MoleTrust2 outperformed random selection only by a small margin but both of them were outperformed by our proposed models. $\mathcal{A}(\mathcal{AR}+\mathcal{I}^2)$ model outperformed both MoleTrust models (despite the latter having some advantage in $F1$) as well as $\mathcal{A}(\mathcal{AR})$ and $\mathcal{A}(\mathcal{I}^2)$. This suggests that average rating and interaction intensity together characterize the ability of trustees reasonably well. $\mathcal{ABIT}(\mathcal{L})$ using trust propensity based on global leniency gave the best overall prediction accuracy among all models. SVM using our 8 features yielded the best performance and was better than $\mathcal{ABIT}(\mathcal{L})$ by merely 0.026. Among the SVM methods, SVM using 8 features did better than SVM13 which uses 13 features not following the Trust Antecedent framework. SVM using all 13 and 8 features did only slightly better than SVM using our 8 features. These results suggest that the Trust Antecedent framework has worked quite well in determining the right trust features for trust ranking. It also demonstrates that the applicability of framework in the online setting.

The second column of Table II shows the weights SVM classifier assigned to our features. Benevolence b_{ji}, surprisingly, was assigned the highest weight. It shows that benevolence a trustee shows to his/her trustors helps to establish trusts among them. On the other hand, trust propensity feature y_i is given a negative weight suggesting that it is not relevant to trust ranking. We suspect that y_i does not capture trust propensity well enough and will investigate this further in our future work.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we apply the trust antecedent framework from management science to develop features under the major factors in trust formation. We propose several trust ranking models using these features. Our experiments show that features derived for all trust factors lead us to new proposed models that perform better than MoleTrust. These features can also be used by SVM to achieve good trust prediction accuracy. Our research shows that trust antecedent framework, despite being qualitative, is useful for trust prediction. Given that trust relationships are important knowledge for the next generation applications, we expect the trust antecedent model to be more commonly adopted for predicting trust in online communities.

REFERENCES

[1] Jennifer Golbeck. Generating predictive movie recommendations from trust in social networks. In *iTrust*, 2006.

[2] Sonja Grabner-Krauter and Ewald A. Kaluscha. Empirical research in on-line trust: A review and critical assessment. *International Journal of Human-Computer Studies*, 58, 2003.

[3] R. Guha, Ravi Kumar, Prabhakar Raghavan, and Andrew Tomkins. Propagation of trust and distrust. In *WWW*, pages 403–412, 2004.

[4] T. Joachims. Making large-Scale SVM Learning Practical. In B. Schölkopf, C. Burges, and A. Smola, editors, *Advances in Kernel Methods - Support Vector Learning*. MIT-Press, 1999.

[5] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *WWW*, 2003.

[6] Matthew K.O. Lee and Efraim Turban. A trust model for consumer internet shopping. *International Journal of Electronic Commerce*, 6(1), 2001.

[7] H. Liu, E.-P. Lim, H. W. Lauw, M.-T. Le, A. Sun, J. Srivastava, and Y. A. Kim. Predicting trusts among users of online communities: an epinions case study. In *ACM EC*, 2008.

[8] P. Massa and P. Avesani. Controversial users demand local trust metrics: An experimental study on epinions.com community. In *AAAI*, 2005.

[9] Yutaka Matsuo and Hikaru Yamamoto. Community gravity: measuring bidirectional effects by trust and rating on online social networks. In *WWW*, 2009.

[10] Roger C. Mayer, James H. Davis, and F. David Schoorman. An integrative model of organizational trust. *Academy of Management Review*, 20:709–734, 1995.

[11] Li Xiong and Ling Liu. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *TKDE*, 16(7), 2004.