Is Trust Transitive and Composable in Social Networks?

Hee Seok Song*

Abstract

Recently, the topic of predicting interpersonal trust in online social networks is receiving considerable attention, because trust plays a critical role in controlling the spread of distorted information and vicious rumors, as well as reducing uncertainties and risk from unreliable users in social networks. Several trust prediction models have been developed on the basis of transitivity and composability properties of trust; however, it is hard to find empirical studies on whether and how transitivity and composability properties of trust are operated in real online social networks. This study aims to predict interpersonal trust between two unknown users in social networks and verify the proposition on whether and how transitivity and composability of trust are operated in social networks. For this purpose, we chose three social network sites called FilmTrust, Advogato, and Epinion, which contain explicit trust information by their users, and we empirically investigated the proposition. Experimental results showed that trust can be propagated farther and farther along the trust link; however, when path distance becomes distant, the accuracy of trust prediction lowers because noise is activated in the process of trust propagation. Also, the composability property of trust is operated as we expected in real social networks. However, contrary to our expectations, when the path is synthesized more during the trust prediction, the reliability of predicted trust did not tend to increase gradually.

Keywords : Trust Propagation, Social Network, Transitivity, Composability, Trust Path, Level of Trust

Received : 2013. 11. 15.　　Revised : 2013. 12. 11.　　Final Acceptance : 2013. 12. 13.

※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology(No. 2010-0020953).

* MIS Department in Hannam University, e-mail : hssong@hannam.ac.kr

1. Introduction

Social networks have played a role to increase the value of social capital through online user interactions that remove geographical boundaries. However, online users in social networks face challenges of assessing whether the anonymous user and his/her provided information is reliable or not because of limited experiences with unknown users. For example, travelers who are reading reviews of hotels often face the situation of judging whether the reviews are posted by hotel marketers pretending to be customers extolling the merit of their hotel. Sometimes online relationships turn sour when one partner in a social network uncovers dramatic misinformation with respect to age or gender [Abdul-Rahman, 2000; Guha et al., 2004]. Uncertainty and concerns about information posted by users and users on the web cannot be solved merely by technical security measures such as integrity, authentication, and non-repudiation, which are developed for e-commerce. An alternative solution for the safe exchange of information and experience among users in social networks is to utilize interpersonal trust among users. Trust plays a critical role in controlling the spread of distorted information and vicious rumors, as well as reducing uncertainties and risk from unreliable users in social networks. As a result, the topic of predicting interpersonal trust is receiving considerable attention in social networks [Bagheri et al., 2009; Jøsang et al., 2006]. In order to predict implicit trust between unknown users, it is vital to provide a successful trust prediction model that builds and maintains a web of trust.

One of the most attempted approaches to establish a trust prediction model among users in social networks is a method based on trust propagation. The trust prediction method (based on trust propagation) is inspired by the concept that trust can be propagated along the friendship chains among users. This method predicts trust by using features of transitivity and composability, which are assumed to be the properties of trust by many previous studies. Transitivity is originated from the fact that people tend to trust the opinions of their friends. Let's suppose that a source user receives a recommendation from his/her friend about an unknown target user. Since the source user trusts the friend, he/she also trusts the unknown target user because the friend trusts the target user. This feature of trust is defined as transitivity. Based on the transitivity property, the trust relationship can be unlimitedly propagated (this is called 'trust path') along the trust chain, which is a direct trust relationship between users [Golbeck, 2005; Guha et al., 2004; Jøsang et al., 2006; Malhotra, 2002; Massa and Avesani, 2006; Ziegler and Golbeck, 2007]. The second property of trust is composability, which means that an unknown target user can be evaluated and trusted through combination of opinions of many people, rather than the opinion of a specific individual who knows the unknown target user. That is, the more a trust path is present from the source user to unknown target user in parallel, the more a reliable evaluation of trust is possible for the target user. This can be similar in real life that it would be more correct to evaluate the reputation of target users from the collection of opinions of multiple friends, instead of relying on the recommendation of one friend.

Recently, several trust prediction models have been developed on the basis of transitivity and composability of trust; however, it is hard to find studies on whether and how transitivity and composability of trust are operated in an actual online social network. According to the previous studies [Golbeck, 2005; Guha et al., 2004; Jøsang et al., 2006; Malhotra, 2002; Massa and Avesani, 2006; Ziegler and Golbeck, 2007], the property of transitivity is always assumed when they build a prediction model for interpersonal trust based on trust propagation. However, there are little empirical studies on whether trust is transitive or not in online social networks. The previous studies for trust prediction also assume the proposition that the farther the distance of trust path between two users is, the lower the correctness of trust prediction becomes in predicting interpersonal trust. For this reason, a discount rate was usually introduced in the trust prediction model so that the recommendation from distant friends can be discounted in trust prediction. In the perspective of a source user, information that a friend of his/hers trusts a target user is more likely to be reliable than information that a friend of the friend of he/she trusts the target user. However, little empirical studies have been conducted on real social network users to investigate how the transitivity operates as it is assumed. Similarly, regarding composability of trust, it is also hard to find the research result verifying that the more trust paths were present in parallel from the source user to an unknown target user, the higher the prediction accuracy of trust becomes. In consequence, this study aims to predict interpersonal trust between two unknown users in social networks and verify the proposition on whether and how transitivity and composability of trust are operated in social networks. For this purpose, we chose three social network sites called Film-Trust, Advogato, and Epinion, which contain explicit trust information by users, and we empirically investigated the proposition.

Our plan for verifying the transitivity and composability properties of trust is to use the prediction accuracy of trust, which is predicted by detour trust path and compared to the direct trust value expressed by the user. High prediction accuracy on trust estimates, which is predicted by the detour trust path, strengthens the hypothesis that the trust is transitive in real social networks because transitivity is defined as 'if A trusts B and B trusts C, then A trusts C'. Similarly, regarding the composability property of trust, if prediction based on multiple trust paths rather than just a trust path toward an unknown target user is more accurate, then it means that the composability operates as expected in real social networks. Therefore, we first built a prediction model for trust, and then investigated whether and how two properties of trust are operated in social networks using prediction accuracy measures. This paper is organized as follows. Section 2 presents the concept of trust and previous studies for predicting trust. Section 3 proposes prediction models for trust to verify the proposition, section 4 discusses our experiments and the results, and finally, section 5 summarizes our work and provides direction for future work.

2. Related Studies

2.1 Concept of Trust

Trust is defined diversely depending on the perspectives of researchers in different academic disciplines. It is defined as 'characteristics of the individual' in psychology, 'estimated risk for reasonable choices of the individual' in economics, and 'part of features of social relationships which are shared between a person with the other person, not individual matters' in sociology. Also, the definition of trust can be divided into psychological and behavioral status depending on the conceptual features. Trust in psychological status is defined as the level of confidence that another person has the goodwill and capability to act out the goodwill [Cook and Wall, 1980], or favorable belief toward another person obtained from a social relationship [Lewicki and Bunker, 1996; Lewis and Weigert, 1985]. Trust also refers to 'a state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of others' [Kim et al., 2008; Mishra, 1996] in behavioral perspective. In this study, trust is defined and used as the concept that is formed through an interactive process of users from the behavioral status. On the other hand, previous studies distinguished types of trust as global and local trust; global trust means objective trust that is property of the trustee regardless of the trust evaluator and illustrated reputation as an example of global trust. However, trust is featured with subjective opinion in terms of the fact that each person can have a different level of trust toward the same target user. Therefore, this study focuses on local trust among users and recognizes it as a subjective measure. Trust can be explicitly expressed by users, or can be measured indirectly through the prediction and monitoring of interactive actions among users.

2.2 Propagation-Based Trust Prediction Studies

The computational model to measure level of trust has been built from security, encryption, authentication, digital signature, P2P system, game theory, agent interaction, recommendation system, and many other areas in computer science since the 1990s. However, studies on trust from social relationships among people have only started recently with the growth of social network services. The main objective of these models is to predict how much a certain user will trust a target user at the end of the trusting chain by mathematically combining several recommendations from trusting users. For this purpose, trust chain and the strength of link are constructed based on a web of trust which consists of explicit trust given by users in a social network.

Golbeck [2005] proposes the TidalTrust algorithm to predict the trust of source users toward target users. In the TidalTrust algorithm, when the source node infers a trust rating for a target user, it asks the source's trusted neighbors for a trust rating for the sink node, and then calculates a weighted average of trust rating from the neighbors to the sink node. This research has shown that highly trusted neighbors and closer neighbors are more accurate in predicting a user's trust value. The TidalTrust algorithm is also strongly affected by the density of a web of trust. If a web of trust is too sparse, it is difficult to find paths from the source to the sink and highly trusted neighbors who have paths to the sink. The TidalTrust model is only applicable to a social network with continuous trust values and confines the search to only the shortest paths when it discovers a trust path. Guha et al. [2004] proposes a trust propagation algorithm which combines distrust with trust and propagates them through a network. The sparsity of a web of trust can be reduced by introducing the concepts of co-citation, transposition of trust, and trust coupling. A relatively low error rate has been observed in predicting trust/distrust between two unknown users. However, it is not always possible to achieve distrust values from users in online social communities. Josang et al. [2006] propose an approach to trust network analysis using subjective logic (TNA-SL), which consists of the three following elements. Firstly, it uses a concise notation with which trust transitivity and parallel combination of trust paths can be expressed. Secondly, it defines a method for simplifying complex trust networks so that they can be expressed in this concise form. Finally, it allows trust measures to be expressed as beliefs, so that derived trust can be automatically and securely computed with subjective logic. This study attempted trust prediction with a new expression system and approaches that had not been introduced in previous studies, and suggested that negative trust propagation could be generated. However, it was limited to present only numerical examples and no comparative evaluation with correctness of prediction, so it is difficult to verify applicability. Although existing studies propose their own algorithms for trust inference based on the assumption of transitivity and composability of trust, there have been no empirical studies to investigate whether and how two properties of trust are operated in an actual online social network.

3. Building Trust Prediction Models

In order to investigate whether and how two properties of trust are operated in an actual online social network, it is required to build a trust prediction model based on trust propagation in advance. The trust propagation-based trust prediction model is composed of a search part for the trust path and a computation part for the level of trust. First of all, the search part of a trust path is performed by an algorithm as seen in <Figure 1>. The search method of a trust path from the source user to target user is performed by Breadth First Search and discovers every possible path, not only the shortest paths. The final output of the algorithm in <Figure 1> is the graph of the web of trust that composes every reachable path from the source user to target user. First, it finds every 1st neighbor in line 1 who directly trusts the target user. In line

```
Input:
$trust\_network\ G = (V, A)$ where a set $V$ is a list of all users and a set $A$ is ordered pairs of users $(u_i, u_j, \tau(u_i, u_j))$
                    $\tau(u_i, u_j)$ is a degree of direct trust value from user $u_i$ toward user $u_j$
source user $u_s$ ; target user $u_t$; a minimum trust threshold $\lambda$

Output:
$trust\_network\ G_{u_s}$ which starts from a source user; $reachable\_inlink\_neighbors$(target user $u_t$)

1. find $N(u_t)$ = users who directly connect to target user $u_t$ (i.e. inlink-neighbors of target uesr $u_t$ ) from $trust\_network\ G$
2. $dist$=0; $trust\_neighbors[dist]$=source user $u_s$;
3. add source user $u_s$ to $trust\_network\ G_{u_s}$;
4. Do while ($trust\_neighbors[dist]$ is not empty)
5.     dist++;
6.     $trust\_neighbors[dist]$= users reachable from $trust\_neighbors[dist - 1]$ and $\forall_j \tau(u_i, u_j) \geq \lambda$;
7.     for each $edge\ (u_i, u_j)$ from $trust\_neighbors[dist - 1]$ to $trust\_neighbors[dist]$
8.         if $(u_i \neq u_j)$ and $\tau(u_i, u_j) \geq \lambda$,
9.         then add $edge\ (u_i, u_j, \tau(u_i, u_j))$ to $trust\_network\ G_{u_s}$;
10.    add all users in $New\_visit$=$\{u_i \mid u_i \in trust\_neighbors[dist]$ and $u_i \notin trust\_neighbors[dist - 1]\}$;
11.    add users in $\{u_i \mid u_i \in New\_visit$ and $u_i \in N(u_i)\}$ into $reachable\_inlink\_neighbors$(target user $u_t$);
12.    reset $trust\_neighbors[dist]$ = users in $\{u_i \mid u_i \in New\_visit$ and $u_i \notin N(u_i)\}$;

13. For each $edge\ (u_i, u_j)$ from $reachable\_inlink\_neighbors$(target user $u_t$) to target user $u_t$
14.    add $edge\ (u_i, u_j, \tau(u_i, u_j))$ to $trust\_network\ G_{u_s}$;
15. add target user $u_t$ to $trust\_network\ G_{u_s}$;
```

<Figure 1> Algorithm for Search and Composing Trust Path

2, it initializes variables that are related to the neighboring group. Next, it adds a source user to the graph of the web of trust (first in line 3) and finds neighbors that the source user trusts before adding to the graph of the web of trust from line 4. At this point, only trust edges exceeding the minimum boundary value are selected (line 6), and trust paths found from line 7 to 9 are added to the graph of the web of trust. The variables are reset to search other neighbors in lines 10 to 12, and links from the first neighbors who trust the target user to the target user are added to the graph of the web of trust in lines 13 to 15; the algorithm is then terminated.

Once every trust path from the source user to target user is found, computation for the level of trust is activated. In the trust computation part, it is necessary to distinguish computational methods for the experiment of transitivity and composability. The reason is that only a trust path is enough to compute the level of trust for the experiment of transitivity on trust, while all the possible trust paths between the source user and target user should be used for the experiment of composability.

3.1 Trust Computation Strategy for the Experiment of Transitivity on Trust

An appropriate computational strategy needs to be chosen among various alternatives in computing the level of trust. The best alternative would be the optimum computational strategy, which would enhance the correctness of trust prediction the most. When we compose computational strategy, the first factor to consider is the types of trust path to use. Golbeck [2005] argued that the shortest trust paths on a trust propagation network are the most desirable paths in computing the level of trust, and suggested the TidalTrust algorithm. The algorithm was based on the assumption that the longer the path reaching to the target user is, the lower reliability of trust prediction becomes. On the contrary, Lesani and Montazeri [2009] and Kim and Song [2011] claimed that using all trust paths from the source to target user can produce a higher accuracy of trust prediction than using only the shortest paths in computing the level of trust. In our experiment, we decided to use all trust paths from the source to target user in computing the level of trust according to the results of Lesani and Montazeri [2009] and Kim and Song [2011].

The second factor to consider is how to compute the final level of trust from individual trust links on a trust path from the source to target user. The first alternative is to use the mean of trust values for each trust link as a final level of trust (T_{mean}) for the trust path from the source to target user. Another alternative, which is more conservative, is to use a minimum trust value among all individual trust links on the trust path as a final level of trust ($T_{\min}$) for the trust path. We adopted these two alternatives to verify the transitivity property of trust. The correctness of trust prediction will be measured by absolute prediction error. Specifically, the predicted trust value, $T(u_s,u_t)$, of source user u_s towards target user u_t will be compared with the actual trust value (direct trust value), $\tau(u_s, u_t)$, to evaluate the correctness of trust prediction and the absolute value of the difference, $\triangle = |T(u_s, u_t) - \tau(u_s, u_t)|$, is defined as prediction error. The overall procedure to verify transitivity property of trust is summarized as follows :

Step 1] Search every trust path which is able to detour for each direct trust link in the test data set, which is necessary to predict the level of trust.

Step 2] Compute the final level of trust (T_{mean} or $T_{\min}$) and absolute prediction error ($\triangle = |T(u_s, u_t) - \tau(u_s, u_t)|$) for each trust path.

Step 3] Group the trust paths according to the paths having the same length and calculate average prediction error according to the length of distance

3.2 Trust Computation Strategy for the Experiment of Composability on Trust

People tend to evaluate trust of others by synthesizing information collected via various routes. Therefore, correctness of trust prediction may vary depending on how diverse trust paths are synthesized on a trust propagation network. In order to verify the trust property of composability, it is needed to decide how to synthesize and calculate the final trust estimates from multiple trust paths between a source and target user. There are two synthesis methods to calculate trust estimates from multiple trust paths; the min-max method and weighted average method. In the min-max aggregation method, it seems reasonable for trust estimates to choose a minimum trust value among all trust values along a trust chain. The longer a chain of trusting users is, the more likely it is to have lower strength of trust path due to the choice of minimum degree of trust. When multiple trust paths are discovered, it is natural to choose a trust path with the highest strength as the best path. The more trust paths that are able to reach the given target user, the more likely it is to have more reliable trust estimates by choosing the trust path with the highest strength. To summarize, min-max method determines the strength of a trust path from the source user to target user as a minimum trust value out of other trust values from trust links on the trust path and uses the highest value of strength of trust path as the value of final trust estimates. On the other hand, Golbeck [2005], and Hyunh and Jennings [2004] suggested a weighted average method to combine multiple evidences of trust. This method is based on the fact that, while the most trustworthy first-hand information (i.e. direct trust value) comes from the strongest paths, weaker paths can also convey valuable information. The weighted average method is to use the average of the direct trust value of first neighbors toward the target user as the final trust estimates, which are weighted by information of strength of trust path from source users to the first neighbor. In the synthesis method of trust path, Kim and Song [2011] showed that the prediction accuracy of combination method with weighted average and min-max method was the best. Therefore, this study tries to synthesize final trust estimates by combination method (T_{cm}) that was obtained from every possible path from source user to target user. Trust $T_{cm}(u_s, u_t)$ of source user u_s toward target user u_t is estimated by the following formula (1) :

$$T_{cm}(u_s, u_t) = \frac{\sum_{u_i \in the\ set\ of\ users\ who\ directly\ trusts\ user\ u_t} ST(u_s, u_i) \times \tau(u_i, u_t)}{\sum_{u_i \in the\ set\ of\ users\ who\ directly\ trusts\ user\ u_t} ST(u_s, u_i)} \qquad (1)$$

In formula (1), trust $T_{cm}(u_s,u_t)$ of source user u_s toward target user u_t is calculated by weighted average of direct trust $\tau(u_i, u_t)$ toward a target user for all first neighbors who directly trust the target user and the strength of trust paths $ST(u_s, u_i)$ from source user to first neighbors is used as weights in this formula. Also, strength of trust paths $ST(u_s, u_i)$ from source user to first neighbor is calculated with the min-max method, as seen in formula (2) :

$$ST(u_s, u_i) = \max_{u_j \in the\ set\ of\ users\ whom\ user\ u_s directly\ trusts} [\min\{\tau(u_s, u_j), ST(u_{j,} u_i)\}] \qquad (2)$$

In formula (2), $\tau(u_s, u_j)$ is the direct trust of user u_s on u_t and a value explicitly expressed by the user u_s. Where, the strength of the trust path is determined with a minimum trust value out of other trust values from trust links on the path, and uses the highest strength of trust path as trust estimates.

Another simpler alternative to compute trust estimates from multiple trust paths will be using simple mean. This method uses the mean of trust value from trust links as the strength of the trust path and the mean of strength from the individual trust path as the final trust estimates (T_{smea}). We adopted these two alternatives to verify the composability property of trust. To verify the hypothesis related to the composability of trust and to carry out the experiment on prediction error for each number of detour paths, the following procedure is proposed.

Step 1] Search every trust path which is able to detour for each trust link in test data set, which is necessary to predict the level of trust.

Step 2] Compute the final level of trust (T_{cm} or T_{smean}) and absolute prediction error ($\triangle = |T(u_s, u_t) - \tau(u_s, u_t)|$) for each trust link in test data set.

Step 3] Group the trust links by the one having the same number of detour paths and calculate the average prediction error according to the number of detour paths.

4. Experiments

To investigate whether and how transitivity and composability of trust are operated in an actual online social network, we applied the proposed prediction models to the website of FilmTrust (http://trust.mindswap.org/FilmTrust), Advogato (http://advogato.org), and Epinion (http://www.epinion.com).

4.1 Data Set

FilmTrust is an online social network that includes movie ratings and movie reviews. FilmTrust allows users to maintain lists of friends and to evaluate how much a user trusts their opinions (i.e. reviews or ratings) about movies. Users assign a degree of trust for their friends from 1 to 10 (i.e. 1 : least trustworthy, 10: most trustworthy). The FilmTrust social network dataset has 571 unique users : 461 users are trusted by at least 1 other user (i.e. trust-inlinks) and 389 users trust at least 1 other user (i.e. trust-outlinks). The dataset has 1,289 trust connections among users. The average of trust values is 6.89 and the median is 7. We set a minimum trust threshold of 8 in our experiments. 791 links out of 1,289 trust links have no detour paths, so these links were excluded and only 498 links were used for trust prediction; prediction error was then calculated.

Advogato is an online community site dedicated to free software development, and also plays the role of a research test bed for testing various trust metrics. In Advogato, users can certify each other on 4 different levels : Observer, Apprentice, Journeyer, and Master; the Advogato trust metric uses this information in order to assign to every user a certification level. Explicitly expressed trust information among users in Advogato has been open on the web in time series since 2000. We chose the snapshot of dataset which was collected at 09：18-2011-Feb-15 and assigned 0 to Observer, 6 to Apprentice, 8 to Journeyer, and 10 to Master to estimate level of trust. The snapshot contains 56,569 trust links, with 4,000 links randomly selected to compose the graph of trust network. The final data set is composed of source user, target user and trust value field, which is explicitly expressed. Selected links contain 1,982 users and the average of trust values is 8.394. We set a minimum trust threshold of 6, then built a web of trust using 4,000 links. After building the web of trust, 800 links out of 4000 links were extracted again to compose the test data set for evaluation of prediction accuracy.

The Epinion dataset allows users to write text reviews and rate other users' reviews with numerical ratings. Epinion also gives a web of trust that would allow a user to express trust of other users based on his/her previous experience. The dataset that was used in our experiment was a snapshot of 2001-Jan-10 and contained 841,372 statements (717,667 trusts and 123,705 distrusts). Columns of this dataset include trustor, trustee, trust value (1 for trust and 0 for distrust), and creation date. Trust is the mechanism by which the user makes a statement that he likes the content or the behavior of a particular user and would like to see more of what the users does on the site. Distrust is the opposite of trust, in which the user says that they want to see lesser of the operations performed by that user (Massa and Avesani, 2006). We chose 4,000 links randomly to compose the graph of trust network among snapshot records. After building the web of trust, all 4000 links were used again to compose the test data set for evaluation of prediction accuracy. The experiments were conducted with a program developed by JAVA program (JDK 1.7) on Intel Core 2 Duo CPU, Windows 7 environment computer.

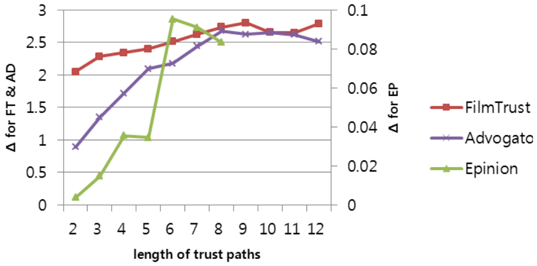
4.2 Experimental Results

We first attempted to verify whether the trust is transitive or not in real social networks. In order to evaluate the property of transitivity, we discovered every detour trust path for each trust link in the test data set and predicted trust estimates then we computed precision $1-\left(\frac{\sum_{i=1}^{n}|T_i(u_s, u_t)-\tau_i(u_s, u_t)|}{n}\right)$ as a measure of prediction accuracy. High precision on trust estimates, which is predicted by the detour trust path, strengthens the hypothesis that the trust is transitive in real social networks because transitivity is defined as 'if A trusts B and B trusts C, then A trusts C'. From Table 1, precision shows above 75% in all cases. Especially in the Epinion dataset, the precision by T_{mean} showed remarkably high values (98.83%). This high precision would be possible because trust has a discrete value in the Epinion dataset. To summarize, <Table 1> presents that the transitivity operates as assumed in real social networks.

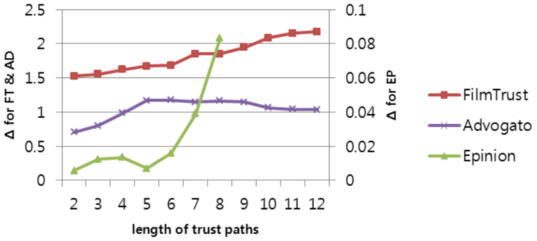
<Table 1> Comparison of Prediction Accuracy

Data set	Predicted by a trust path	
	Precision by $T_{\min}$	Precision by T_{mean}
FilmTrust	75.29%	82.58%
Advogato	78.08%	89.65%
Epinion	97.27%	98.83%

The additional experimental result to verify transitivity property is presented in <Figure 2> and <Figure 3>. <Figure 2> and <Figure 3> show average prediction error according to the length of trust path. The average prediction error shown in <Figure 2> is derived from $T_{\min}$, which is set by a minimum trust value among all individual trust links on the trust path, while those in <Figure 3> are derived from T_{mean}, which uses a mean of trust values belonging to individual trust links as the final estimates of trust. From <Figure 2> and <Figure 3>, we can determine a trend that the longer the length of a path, the higher the prediction error. To test increasing trends of prediction error statistically, linear regression model was applied. The result showed that beta coefficient for path distance took a positive value (0.120 in Advogato, 0.065 in FilmTrust), and the significance level was 0.0. Therefore, there is a significant positive correlation between the increase of path distance and increase of prediction error. This increasing trend of prediction error supports the proposition that the farther the trust path between two users becomes, the lower the reliability of predicted trust information becomes. Therefore, using discount rates in the trust prediction model is desirable because the recommendation from distant friends can be discounted in trust prediction. In other words, this result also supports prior expectations that information for a source user that a friend of his/hers trusting a target user is more likely to be reliable than information that a friend of the friend of he/she trusts the target user.



〈Figure 2〉 Prediction Error According to the Path Length ($T_{\min}$)



〈Figure 3〉 Prediction Error According to the Path Length (T_{mean})

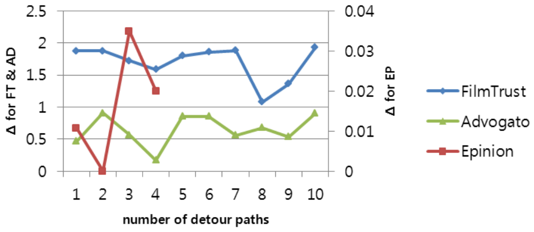
Similarly, regarding the composability property of trust, we compared prediction errors for each prediction strategy. <Table 2> shows the overall prediction error for each strategy. If prediction based upon multiple trust paths rather than just a trust path toward an unknown target user is more accurate, it means that the composability operates as expected in real social networks. In <Table 2>, prediction errors predicted from a trust path are higher than those from multiple trust paths in all three data sets. This result means that the composability property of trust also operates as we expected in real social networks.

However, more investigation is needed to verify the proposition that the more trust paths are present in parallel from the source user to an unknown target user, the higher the prediction accuracy of trust becomes. For this purpose, additional experimentation is conducted to

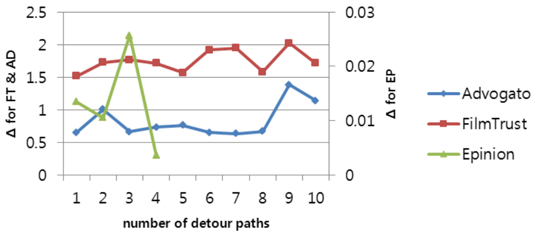
<Table 2> Comparison of overall prediction error

Data set	Predicted by a trust path			Predicted by multiple trust paths		
	$\triangle by\ T_{\min}$	$\triangle by\ T_{mean}$	Sum	$\triangle by\ T_{cm}$	$\triangle by\ T_{smean}$	Sum
FilmTrust	2.4709	1.7420	**4.2129**	1.8355	1.6876	**3.5231**
Advogato	2.1919	1.0348	**3.2267**	0.6886	0.8671	**1.5557**
Epinion	0.0273	0.0117	**0.0390**	0.0125	0.0122	**0.0247**

identify whether the prediction error changes according to the number of trust paths.



<Figure 4> Prediction Error According to the Number of Paths (T_{cm})



<Figure 5> Prediction Error According to the Number of Paths (T_{smean})

In <Figure 4> and <Figure 5>, there is no decreasing trend of prediction error according to the increment number of paths. In other words, even though the more paths are synthesized during the trust prediction, the prediction error does not reduce gradually. This is an unexpected result against previous expectations that people tend to evaluate trust of others by synthesizing information collected via various routes. The reason would be that if path distance is long, path combination increases and the number of paths also increases. The result of Pearson's correlation coefficient between the actual number of paths and path distance in Advogato data set showed 0.654 (significance level : 0.0), which is a strong correlation. In other words, it was expected that if a prediction was made by synthesizing a larger number of paths, prediction error might be reduced. However, a larger number of paths means a longer path distance. Therefore, it is understood that an increased number of paths, which causes decreased prediction error, has an offset effect with the increase of path length, which in turn, increases prediction error. To sum up, prediction error is lower when paths are synthesized than when an individual path is used for trust prediction. However, the trend was not found that an increased number of paths used in synthesizing causes prediction error to lower.

5. Conclusion

This study experimented with data sets of three social network sites called FilmTrust, Advogato, and Epinion to verify whether the transitivity and composability properties of trust operates in real social network sites, and how those properties are operated on social networks. Experimental results showed that as path distance increases, prediction error tends to significantly increase. This means that trust can be propagated farther and farther along the trust link, however, when path distance becomes distant, correctness of trust prediction becomes lower since noise is activated in the process of trust propagation. Therefore, when path distance becomes longer, the most desirable prediction method would be applying discount rates in trust prediction. On the other hand, experimental result on the correctness of trust prediction by the number of trust paths showed that the prediction errors predicted from a trust path are higher than those from multiple trust paths in all three data sets. This result means that the composability property of trust is also operated as we expected in real social networks. However, contrary to our expectations, the more the path is synthesized during the trust prediction, the prediction error does not tend to reduce gradually. It is understood that an increased number of paths, which decreases prediction error, has an offset effect with the increase of path length, which increases prediction error. In other words, correctness increases in trust prediction when various detour paths are synthesized than when predicted by an individual path; however, a simple increase of trust paths does not mean an increase of the correctness of trust prediction.

This study was verified with experiments conducted in social networks on transitivity and composability of trust propagation that had been assumed in previous studies. The results of this study are expected to contribute in terms of suggesting guidelines to improve correctness in trust prediction based on trust propagation, because trust inference quality through trust propagation is affected by the length of trust paths and different aggregation approaches, which decide how to combine multiple information sources. As a further research area, it is necessary to apply the results to more data sets and generalize the results. It would also be an interesting topic to identify the differences in results according to the value type of trust such as discrete or continuous. Additionally, more extensive experiments with a larger-scale dataset need to be carried out. Finally, trust is situational and dependent upon various factors. For example, A can trust B in film choice, but A may not trust B in car mechanic service recommendation. It means that situational factors can be added to identify transitivity and composability of trust paths in further studies.

References

[1] Abdul-Rahman, S. Hailes, "Supporting trust in virtual communities", *Proceeding of HICSS' 00*, 2000, pp. 6007-6008.

[2] Bagheri, E., Zafarani, R., and Barouni-Ebrahimi, M., "Can reputation migrate? On the propagation of reputation in multi-context communities", *Knowledge-based systems*, Vol. 22, No. 6, 2009, pp. 410-420.

[3] Cook, J. and Wall, T., "New work attitude measures of trust, organizational commitment and personal need non-fulfilment", *Journal of Occupational Psychology*, Vol. 53, 1980, pp. 39-52.

[4] Golbeck, J., "Computing and applying trust in web-based social networks", Doctor of C.S. dissertation, University of Maryland, 2005.

[5] Golbeck, J., "Weaving a Web of Trust", *Science,* Vol. 19, 2008, pp. 1640-1641.

[6] Guha, R., Kumar, P., and Raghavan, A., "Propagation of trust and distrust", *International World Wide Web Conference*, 2004, pp. 403-412.

[7] Huynh, T. D., Jennings, N. R., and Shadbolt, N. R., "Developing an Integrated Trust and Reputation Model for Open Multi-Agent Systems", *7th International Workshop on Trust in Agent Societies*, 2004.

[8] Jøsang, A., Gray, E., and Kinateder, M., "Simplification and analysis of transitive trust networks", *Web Intelligence and Agent System*, Vol. 4, No. 2, 2006, pp. 139-161.

[9] Kim, Y. A., Le, M.-T., Lauw, H. W., Lim, E.-P., Liu, H., and Srivastava, J., "Building a Web of trust without explicit trust ratings", *Data Engineering Workshop (ICDEW 2008)*, 2008, pp. 531-536.

[10] Kim, Y. A. and Song, H. S., "Strategies for predicting local trust based on trust propagation in social networks", *Knowledge-Based Systems*, Vol. 24, 2011, pp. 1360-1371.

[11] Lesani, M. and Montazeri, N., "Fuzzy trust aggregation and personalized trust inference in virtual social networks", *Computational Intelligence*, Vol. 25, No. 2, 2009, pp. 51-83.

[12] Lewicki, R. J. and Bunker, B. B., "Developing and Maintaining Trust in Work Relationships", *Trust in Organizations : Frontiers of Theory and Research*, 1996, pp. 114-139.

[13] Lewis, J. D. and Weigert, A., "Trust as a Social Reality", *Social Forces*, Vol. 63, 1985, pp. 967-985.

[14] Malhotra, R. and Malhotra, D. K. R., "Differentiating between good credits and bad credits using neuro-fuzzy systems", *European journal of operational research,* Vol. 136, 2002, pp. 190-211.

[15] Massa, P. and Avesani, P., "Trust-aware bootstrapping of recommender systems", *Proceedings of ECAI 2006 Workshop on Recommender Systems,* 2006, pp. 29-33.

[16] Mishra, A. K., "Organizational Responses to Crisis : The Centrality of Trust, Trust in Organization", London : Sage, 1996.

[17] Song, S., Hwang, K., Zhou, R., and Kwok, U.-K., "Trusted P2P Transactions with Fuzzy Reputation Aggregation", *IEEE Internet Computing,* 2005, pp. 18-28.

[18] Ziegler, C.-N. and Golbeck, J., "Investigating correlations of trust and interest similarity", *Decision Support Systems*, Vol. 43, No. 2, 2007, pp. 460-475.

■ Author Profile

Hee Seok Song

Song, Hee Seok is a professor of management information systems department at Hannam University in Korea. He received bachelor's degree from Korea University and PhD degree from Korea Advanced Institute of Science and Technology. His research interests include intelligent computing technology, business intelligence, and social network.

◈ "본 논문은 한국정보기술응용학회 한국데이타베이스학회 2013년 공동추계학술대회에서 발표된 논문으로서 JITAM 논문지 편집위원회의 심사과정을 거쳐 본 호에 게재함."