Trust Prediction Using Positive, Implicit, and Negative Information

Min-Hee Jang
Computer Science Dept.
Carnegie Mellon University
Pittsburgh, USA
zzmini@cs.cmu.edu

Christos Faloutsos
Computer Science Dept.
Carnegie Mellon University
Pittsburgh, USA
christos@cs.cmu.edu

Sang-Wook Kim
Dept. of Computer Science and Engineering, Hanyang University, Seoul, Korea
wook@hanyang.ac.kr

ABSTRACT

We propose a novel method to predict accurately trust relationships of a target user even if he/she does not have much interaction information. The proposed method considers positive, implicit, and negative information of all users in a network based on *belief propagation* to predict trust relationships of a target user.

Categories and Subject Descriptors

H.2.8 [**Database Management**]: Database applications—*Data mining*

General Terms

Experimentation, Measurement

Keywords

Trust prediction, Belief propagation,Trustworthiness

1. INTRODUCTION

Trust prediction methods, which predict future trust relationships of users, have been proposed to find trustable users in social networks [1][2][3]. In social networks, users explicitly make *trust* and *distrust* relationships with other users and *rate* other users' contents as well. These activities are called *interaction information* between users [2][3].

Most previous methods for link prediction infer trust relationships between two users based on the interaction information. In case two users have not much interaction information, the previous methods cannot infer the trust relationship. Also, they use only partial information of the interaction, thereby being difficult to predict trust relationships.

To solve the problem, we propose a novel trust prediction method using *belief propagation* (BP) [4]. The proposed method measures each user's trustworthiness for a target user by using the interaction information of all users. Also, the proposed method considers *all types of interaction information*, the trust, distrust, and ratings, to measure the trustworthiness accurately. We show the effectiveness of the proposed method via a series of experiments.

WWW'14 Companion, April 7–11, 2014, Seoul, Korea.
ACM 978-1-4503-2745-9/14/04.
http://dx.doi.org/10.1145/2567948.2577288.

2. THE PROPOSED METHOD

BP is an algorithm that infers the state of a node by computing the *belief score* of the node [4]. The belief score of a node means the probability which the node is in a specific state. In this paper, two states of a node are defined: <*trustable*, *distrustful*>. The belief score of a node is computed by exchanging *messages* between nodes. The message is a node's opinion about a neighboring node's possibility of being in a specific state. The messages sent from one node to a neighbor are represented as a vector. The elements of the vector are the two states of a node mentioned above. Each message that node u_i sends to node u_j is computed as follows:

$$m_{ij}(x_p) \leftarrow \sum_{x_q \in X} \phi_i(x_q)\psi(x_q, x_p) \prod_{k \in N(i) \setminus j} m_{ij}(x_q) \qquad (1)$$

In this equation, two states x_p and x_q exist. $m_{ij}(x_p)$ represents the message that u_i sends to u_j, indicating u_i's opinion about u_j's probability of being in state x_p. $\phi_i(x_q)$ is a *prior belief* which means the probability of u_i being in state x_q. $\psi_{ij}(x_q,x_p)$ is the probability of u_j being in state x_p when u_i is in state x_q. It is defined by the *propagation matrix*.

$m_{ij}(x_p)$ is computed with the product of the messages from u_i's neighbors except u_j. It is computed iteratively for a specific number of times or until the message value is converged [4]. After the computation, the belief scores of each node are computed. The belief scores are represented as a vector with the two states as well. Each belief score is computed as follows. k is a normalization factor.

$$b_i(x_p) = k\phi_i(x_p) \prod_{j \in N(i)} m_{ji}(x_p) \qquad (2)$$

To apply BP to the trust prediction, we construct a network where nodes and directed edges indicate users and interactions between users. The network has two types of edges: the positive and negative edges. The positive edge is created when a user makes a trust relationship with another user and/or rates another user's content. The negative edge is created when a user makes a distrust relationship with another user.

After constructing a network, we should assign the prior beliefs of each node. If the prior belief on the trustable state of node u_i is high, the message on the trustable state of u_i would be also high. As a result, the node nearer to u_i gets the higher belief score. In this paper, we assign the prior beliefs of all other nodes as <0.5+α , 0.5–α> (α: very small number) and those of the target node as <0.5+α', 0.5–α'> ($\alpha' \gg \alpha$) to give the higher belief score to the node nearer

to the target node. To compute the belief score, we define two propagation matrixes in Table 1(a) and Table 1(b) for the positive and negative edges related to $\psi_{ij}(x_q,x_p)$.

Table 1: Propagation matrixes

(a) Positive edge

Positive		Destination	
		Trust	Distrust
Source	Trust	$0.5+\varepsilon(t+f(r))$	$0.5-\varepsilon(t+f(r))$
	Distrust	$0.5-\varepsilon(t+f(r))$	$0.5+\varepsilon(t+f(r))$

(b) Negative edge

Negative		Destination	
		Trust	Distrust
Source	Trust	$0.5-\varepsilon$	$0.5+\varepsilon$
	Distrust	$0.5+\varepsilon$	$0.5-\varepsilon$

In $\psi_{ij}(x_q,x_p)$, the column (source) represents x_q and the row (destination) represents x_p. For example, in the positive edge, $\psi_{ij}(trustable, trustable)$, the probability of a destination node u_j being in state *trustable* when a source node u_i is in state *trustable* is $0.5+\varepsilon(t+f(r))$. ε controls the influence of the source on the destination. t is a binary parameter to represent the existence of trust relationship between two users. If a trust relationship exists, $t=1$, otherwise $t=0$.

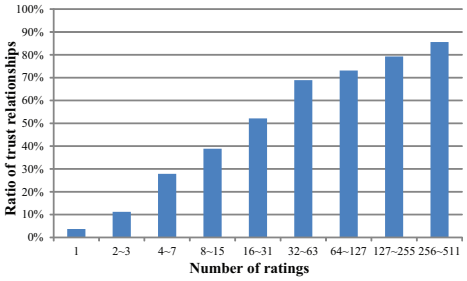

Figure 1: Ratio of trust relationships with respect to the varying number of ratings.

$f(r)$ is the trust degree measured by the number of ratings from source node u_i to destination node u_j. If u_i gives more ratings to u_j, u_i is more likely to trust u_j [3]. We examine the correlation between the number of ratings and the existence of trust relationship in a user pair by using *Epinions.com* data. Figure 1 shows the result. The x-axis indicates the number of ratings in a user pair and the y-axis does the probability of the user pair having a trust relationship. As the number of ratings increases, the probability also increases. Based on this observation, the proposed method estimates $f(r)$ as shown in Table 2.

Table 2: $f(r)$ with a varying number of ratings

Ratings	1	2~3	4~7	8~15	16~31	32~63	64~127	127~255	265~511
f(r)	0.04	0.09	0.29	0.39	0.52	0.68	0.75	0.78	0.85

In the propagation matrix of the negative edge, $\psi_{ij}(trustable, trustable)$ is $0.5-\varepsilon$. This is because ordinary users usually want to avoid distrustful users [2][3]. The proposed method computes the belief score of each node in a network using the prior belief and the propagation matrixes, and returns the k nodes that have the highest belief scores as a prediction result for the target user.

3. EXPERIMENTS

In our experiments, we compared the accuracy of the proposed method with two existing methods, *ITD* [3] and *ABIT_L* [2]. The data used in our experiments is Epinions.com data that contains 131,828 users, 717,667 trust relationships, 123,705 distrust relationships, and 13,668,319 ratings [1]. Parameters of the proposed method were set as follows: $\alpha=0.0001$, $\alpha'=0.1$, $\varepsilon=0.005$.

To measure the accuracy of each method, we first randomly selected a target user who rated other users less than 50 times and has trust relationships less than 20. Then, we deleted the target user's existing k trust relationships ($k=$ 25%, 50%, 75%, 100%). After that, the proposed method computes the belief score of each node and the previous methods compute the probability of making trust relationships between the target node and every other nodes in the network. For each method, the computed values for all the nodes are sorted in descending order and the top k nodes from the sorted list are selected as predicted results. The accuracy is a ratio of correct predictions to all the predictions.

Figure 2 shows the results. Compared to *ITD* and *ABIT_L*, our method has higher accuracy by up to 10.1% and 20.6%, respectively. The proposed method measures each user's trustworthiness for the target user instead of inferring the relationship. Also, our method uses all types of interaction information, the trust, distrust, and ratings, thereby predicts trust relationships more accurately.

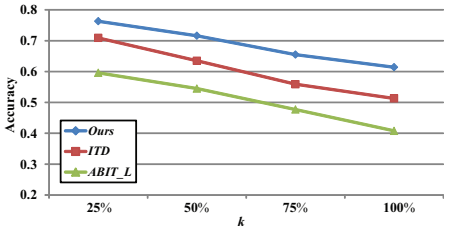

Figure 2: Accuracy comparison.

4. CONCLUSION

In this paper, we have proposed a novel BP-based method to predict the trust relationship of a target user. The experimental results show that our method significantly outperforms previous methods in terms of the accuracy.

5. ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No.CNS-1314632 and by the Army Research Laboratory under Cooperative Agreement Number W911NF-09-2-0053. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation, or other funding parties. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on. This research is also supported by the MSIP (The Ministry of Science, ICT and Future Planning), Korea and Microsoft Research, under IT/SW Creative research program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2013-H0503-13-1029) and by Basic Science Research Program through the NRF funded by the Ministry of Education, Science and Technology (No. 2013R1A6A3A03027153).

6. REFERENCES

[1] P. Massa and P. Avesani. Controversial users demand local trust metrics: an experimental study on epinions.com community. In *Proc. National Conf. on AAAI*, pages 121–126, 2005.

[2] V. Nguyen, E. Lim, J. Jiang, and A. Sun. To trust or not to trust? predicting online trusts using trust antecedent framework. In *Proc. Int'l. Conf. on ICDM*, pages 896–901, 2009.

[3] H. Oh, J. Kim, S. Kim, and K. Lee. A probability-based trust prediction model using trust-message passing. In *Proc. Int'l. Conf. on WWW*, pages 161–162, 2013.

[4] J. Yedidia, W. Freeman, and Y. Weiss. *Understanding belief propagation and its generalizations.* Morgan Kaufmann Publishers Inc., 2003.