IoT Service Provider Recommender Model Using Trust Strength

Weiwei Yuan[1,2], Chenliang Li[1], Donghai Guan[1,2], Guangjie Han[3](✉), and Feng Wang[4]

[1] College of Computer Science and Technology,
Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
{yuanweiwei,dhguan}@nuaa.edu.cn, lcljoric@gmail.com
[2] Collaborative Innovation Center of Novel Software Technology
and Industrialization, Nanjing 210093, China
[3] Deparment of Information and Communication Systems, Hohai University,
Changzhou, China
hanguangjie@gmail.com
[4] School of Information Science and Engineering, Changzhou University,
Changzhou 213164, China
wfeng@cczu.edu.cn

Abstract. Recommendation algorithms predict users' opinions towards IoT service providers, helping users finding things that might be of their interests. With the rapid development of IoT applications, various recommender models have been proposed for usage, trust-aware recommender models have been verified to have reasonable recommendation performances even in case of data sparseness. However, existing works did not consider the influence of distrust between users. They recommend items only base on the trust relations between users. We therefore propose a novel trust strength based IoT service provider recommender model which predicts ratings with recommendations given by recommenders with both trust and distrust relations with the active users. The trust strength also merges both local and structural information of users in the trust network. The experimental results show that the proposed method has better prediction accuracy and prediction coverage than the existing works. In addition, the proposed method is computational less expensive.

Keywords: Service provider recommendation
Trust-aware recommendation algorithm · Recommender systems

1 Introduction

Recommendation algorithms predict users' opinions towards service providers of IoT, helping users finding things that might be of their interests. With the rapid development of IoT [1], it is more and more important for IoT applications to find the reliable IoT service providers for users. Trust-aware Collaborative Filtering (TCF) [3, 4] improves the classical Collaborative Filtering (CF) [2] by exploiting users' trust to predict their ratings on service providers. TCF merges the recommendations according to the trust relations between the active user and the recommenders. Since trust is transitive, it is

Y.-B. Lin et al. (Eds.): IoTaaS 2017, LNICST 246, pp. 286–293, 2018.
https://doi.org/10.1007/978-3-030-00410-1_34

possible to build up the relationship between users via trust propagations. This makes TCF have good recommendation performances in case of data sparseness.

However, existing TCF models recommend items only based on trust relations between users. They did not consider the influence of distrust between users. This is because trust relations is easier to be calculated than the distrust relations. Trust is transitive, while distrust is not transitive. Furthermore, it is also not easy to merge the trust relations and the distrust relations directly. Since trust relations always coexist with distrust relations in the real applications, ratings should be predicted with the recommendations given by users with both trust and distrust relations.

To solve the problems of existing works, we propose a novel trust strength based IoT service provider recommender model. The trust strength merges local information and structural information of the users in a social network with both trust relations and distrust relations. Logistic Regression is used to calculate the trust strength and the recommendations are then merged by the trust strength to give the prediction. The experimental results show that the proposed method has better prediction performances comparing with the existing works. In addition, the proposed method is computational less expensive.

The contributions of this work mainly lie in: (1) The proposed method involves both trust and distrust relations between users to predict ratings. This makes it more suitable to be applied in the real applications. (2) The proposed method considers both local and structural information of users in the trust network to predict ratings. This makes it more appropriate to reflect the real trust strength between users. (3) The proposed method is computational much less expensive than the existing works.

The rest of the paper is organized as follows: Sect. 2 describes the related works, Sect. 3 introduces the proposed method, Sect. 4 demonstrates the experiment results, and the last section concludes this paper and points out the future works.

2 Related Works

This paper proposes a trust strength based recommender model for IoT service provider recommendation. It is closely related to TCF [3, 4] which predicts ratings with only trust relations. The rating prediction mechanism of TCF is similar to that of CF [2]:

$$p_{act,i} = \overline{r_{act}} + \frac{\sum_{rec=1}^{k} w_{act,rec}\left(r_{rec,i} - \overline{r_{rec}}\right)}{\sum_{rec=1}^{k} w_{act,rec}}, \tag{1}$$

where $p_{act,i}$ is the predicted rating of the active user act on item i, rec is one of the k recommenders who have rated i, $\overline{r_{act}}$ and $\overline{r_{rec}}$ are the average rating of act and rec respectively, $r_{rec,i}$ is the recommendation given by rec on i, and $w_{act,rec}$ is the weight of act on rec . $w_{act,rec}$ is calculated as:

$$w_{act,rec} = \frac{d_{\max} - d_{act,rec} + 1}{d_{\max}}, \tag{2}$$

where $d_{\max}$ is the maximum allowable trust propagation distance, and $d_{act,rec}$ is the trust propagation distance from *act* to *rec*, $d_{act,rec} \leq d_{\max}$. As shown in (2), TCF only involves trust relationships between users.

There are also some other recommender models related to the proposed method including CF+TCF [4], which utilizes the basic model of CF while calculating the weight by combining users' similarities and trust relations; UPC [9], which uses a user preference clustering method to substitute the neighbor finding and weight assigning mechanism of CF; RTCF [10], which utilizes the basic model of TCF while uses the reliability score to reconstruct the trust network before finding neighbors; RDT [11], which combines user ratings and trusts as a neighbor finding mechanism.

The proposed method involves both trust and distrust relations in trust strength calculation. Since distrust cannot propagate, trust and distrust are merged according to the Structural Balance Theory [5] in this work. Structural Balance Theory focuses on the triad relations between users. It predicts social relations between users to keep the balance of triangles involved in trust networks. Structural Balance Theory considers the triad social relations between users as undirected networks. Two kinds of triad relations are regarded as balanced by the Structural Balance Theory, as shown in Fig. 1. The balanced triangles should have either three trust relationships or one trust relations and two distrust relationships. Other triangles are all regarded as unbalanced. The proposed method involves the distrust information to calculate the trust strength to keep the balance of triangles including the active users and the recommenders. Note that to simplify the calculation of trust strength, this work regards the involved triads as undirected triads.

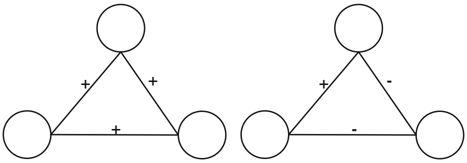

Fig. 1. Balanced triad relationships according to the Structural Balance Theory.

3 The Proposed Method

The architecture of the proposed method is given in Fig. 2. The proposed IoT service provider recommender model consists of three modules: the feature selection module, the trust strength calculation module and the rating prediction module. The details of the proposed method are as follows.

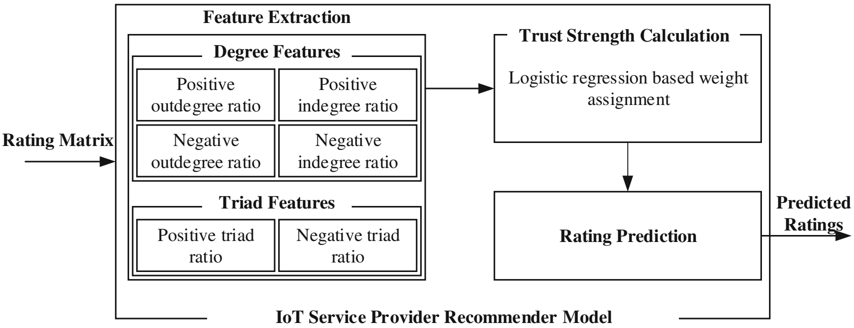

Fig. 2. The architecture of the proposed method.

(1) Feature Extraction

To calculate the trust strength between users, two kinds of features are extracted:

(A) Degree features

A user's degree represents its local trust relations with other users. Let *act* be an active user and *rec* be a recommender. Four degree features are extracted to evaluate a recommender's trust strength on the active user, which include the positive outdegree ratio of *act* $POR(act)$, the negative outdegree ratio of *act* $NOR(act)$, the positive indegree ratio of *rec* $PIR(rec)$, and the negative indegree ratio of *rec* $NIR(rec)$:

$$POR(act) = \frac{d_{out}^{+}(act)}{d_{out}^{+}(act) + d_{out}^{-}(act)} \tag{3}$$

$$NOR(act) = \frac{d_{out}^{-}(act)}{d_{out}^{+}(act) + d_{out}^{-}(act)} \tag{4}$$

$$PIR(rec) = \frac{d_{in}^{+}(rec)}{d_{in}^{+}(rec) + d_{in}^{-}(rec)} \tag{5}$$

$$NIR(rec) = \frac{d_{in}^{-}(rec)}{d_{in}^{+}(rec) + d_{in}^{-}(rec)} \tag{6}$$

where $d_{out}^{+}(act)$ is the positive outdegree of *act*, $d_{out}^{-}(act)$ is the negative outdegree of *act*, $d_{in}^{+}(rec)$ is the positive indegree of *rec*, and $d_{in}^{-}(rec)$ is the negative indegree of *rec*.

The higher value $POR(act)$ has, the more likely *act* will trust other users, and the more likely there exists tight trust strength between *act* and *rec*. The higher value $NOR(act)$ has, the more likely *act* will distrust other users, and the less likely there exists tight trust strength between *act* and *rec*. The higher value $PIR(rec)$ has, the more likely *rec* will be trusted by other users, and the more likely there exists tight trust strength between *act* and *rec*. The higher value $NIR(rec)$ has, the more likely *rec* will be distrusted by other users, and the less likely there exists tight trust strength between *act* and *rec*.

(B) Triad features

According to the Structural Balance Theory, the trust relations between users are also related to the triad relationship of the trust network. The triangles in the social network represent the structural information related to the target user. The balanced triangles of the trust network are given in Sect. 2. Two triad features are extracted to evaluate the trust strength between users, which include the positive triad ratio $PTR(act, rec)$ and the negative triad ratio $NTR(act, rec)$ between *act* and *rec*:

$$PTR(act, rec) = \frac{\sum\limits_{comNei \in C} I(Sign(act, comNei) * Sign(rec, comNei) = 1)}{|C|} \tag{7}$$

$$NTR(act, rec) = \frac{\sum\limits_{comNei \in C} I(Sign(act, comNei) * Sign(rec, comNei) = -1)}{|C|} \tag{8}$$

where C represents the set of common neighbors between *act* and *rec*, $|C|$ is the number of common neighbors between *act* and *rec*, and $I(.)$ is an indicator function which equals to 1 if the equation inside is true.

Considering the triangle consisting the active user *act*, the recommender *rec* and one of their common neighbor *comNei*, if the sign of the social relations between *act* and *comNei* is the same as the sign of the social relations between *rec* and *comNei*, the social relation between *act* and *comNei* should be positive to keep the balance of the triangles. These triangles are named as positive triad in this work. While if the sign of the social relations between *act* and *comNei* is the opposite to the sign of the social relations between *rec* and *comNei*, the social relation between *act* and *comNei* should be negative to keep the balance of the triangles. These triangles are named as negative triad in this work. The higher value $PTR(act, rec)$ has, the more likely there exists a tight trust strength between *act* and *rec*; while the higher value $NTR(act, rec)$ has, the less likely there exists a tight trust strength between *act* and *rec*.

(2) Trust Strength Calculation

Based on the above features representing the degree information and the triad information, trust strength between the active user and the recommender is calculated. The influence of these selected features is calculated by a non-linear model:

$$s = \frac{1}{1 + e^{-(\mathbf{w}^T \mathbf{x} + b)}} \tag{9}$$

where s denotes the trust strength, $\mathbf{w}$ denotes the array of the weights assigned to the extracted features, $\mathbf{x}$ is the array of features, and b is a constant. The parameter $\mathbf{w}$ is calculated by Logistic Regression, which aims at optimizing the following objective function:

$$\min_{\mathbf{w},b} \alpha\|\mathbf{w}\|_2^2 + \sum\nolimits_{i=1}^{n} \ln\left(e^{-y_i(\mathbf{w}^T\mathbf{x}_i + b)} + 1\right) \tag{10}$$

where y_i equals to 1 if the i^{th} link of the training set is the trust relationship, y_i equals to 0 if the i^{th} link of the training set is the distrust relationship, $\mathbf{w}^T\mathbf{w}$ is a regularizer, and α is a parameter determining the significance of the regularizer. The parameter $\mathbf{w}$ is then calculated by performing gradient descent method or Newton method.

(3) Rating Prediction

Using the trust strength calculated by (9), the active user's rating on the target item i is calculated as follows:

$$p_{act,i} = \frac{\mathbf{s} \cdot \mathbf{r}}{\|\mathbf{s}\|_1} \tag{11}$$

where $\mathbf{s}$ is the array of trust strength between the active user and the recommenders, and $\mathbf{r}$ is the array of recommendations on the target item.

4 Experimental Results

Experiments are held on two datasets to verify the performances of the proposed method. The datasets are extracted from the online review website Epinions. The Epinions dataset [8] has 13,668,320 user-item ratings. Users in the Epinions dataset connect to others by trust and distrust links in the user-user trust network. We randomly extract 300,000 ratings from the Epinions dataset as the basis of the experimental dataset. Trust between the users giving these ratings are then extracted from the Epinions dataset to measure the social relationship between users. This dataset is called the original dataset in the experiments. To examine the performances of the proposed method in case of sparse trust relations, a dataset named sparse trust dataset is extracted from the original dataset. In the sparse trust dataset, 70% of the social relations, which include trust and distrust, are randomly removed from the social relations of the original dataset. Two kinds of performances are examined for the proposed method. One is the prediction accuracy of the proposed method, which is calculate by the Mean Absolute Error (MAE). And the other is the prediction coverage of the proposed method.

Based on the experimental results, the prediction performances of the proposed method using the original dataset and the sparse trust dataset are given in Figs. 3 and 4 respectively. It is shown that the prediction accuracy of the proposed method is better than the prediction accuracy of the existing works by using both the original dataset and the sparse trust dataset. Though the prediction accuracy of UPC is slightly worse than that of the proposed method, the prediction coverage of the proposed method is significantly higher than UPC by using the original dataset and sparse trust dataset. The coverage of the proposed method is better than that of the existing works by using the original dataset and the sparse trust dataset. Among the existing works, the prediction coverage of RDT is the best, which is only slightly worse than the prediction coverage of the proposed method.

However, the prediction accuracy of the proposed method is significantly better than that of RDT by using the original dataset and sparse trust dataset.

The computational complexity of the proposed method is measured by the time consumption in this work. Figure 5 gives the time consumption of the proposed method comparing with that of the existing works. By using both the original dataset and the sparse trust dataset, the time consumption of the proposed method is significantly less than that of the existing work. This means the computational complexity of the proposed method is the lowest among all works.

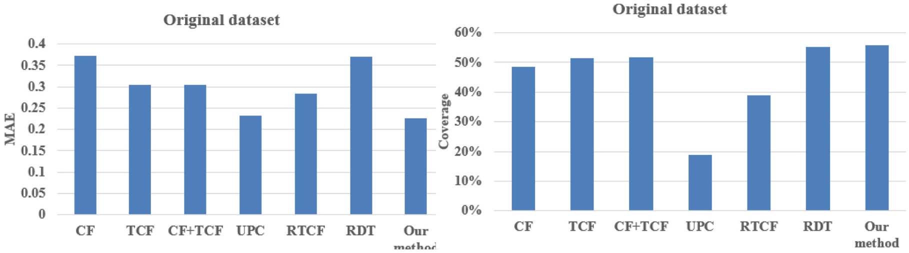

Fig. 3. The prediction performances of the proposed method by using the original dataset.

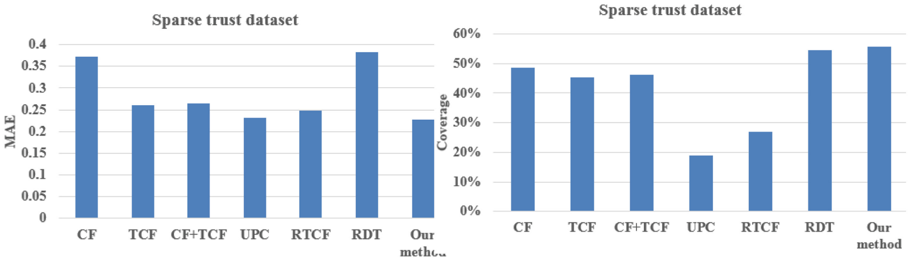

Fig. 4. The prediction performances of the proposed method by using the sparse trust dataset.

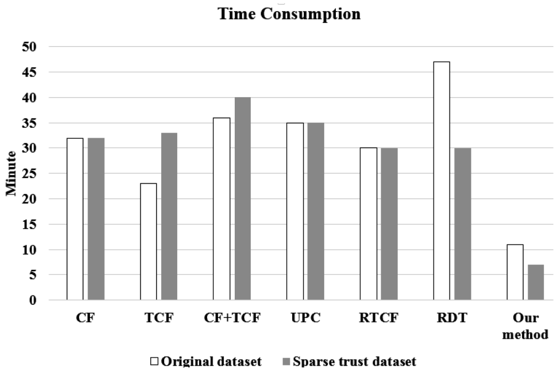

Fig. 5. The time consumption of the proposed method by using the original dataset and the sparse trust dataset.

5 Conclusion and Future Works

This paper aims at proposing an IoT service provider recommender model which would reliably recommend service providers to the users of IoT. This is achieved by recommending IoT service providers based on the trust strength between users. The proposed work involves both trust and distrust relations between users. It also involves both local and structural information of users in trust networks. Experiments results show that the proposed method has better prediction performances than existing works. Our future research will mainly focus on developing more high-performance recommendation algorithms exploiting trust and distrust information. We also plan to apply the proposed trust strength based recommender model in more application areas, e.g., in the applications mentioned [6, 7]. This would further improve the performances of the proposed model in real applications.

Acknowledgements. This research was supported by Nature Science Foundation of China No. 61672284, Natural Science Foundation of Jiangsu Province of China No. BK20171418, Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China No. CAAC-ITRB-201501 and No. CAAC-ITRB-201602, China Postdoctoral Science Foundation No. 2016M591841 and No. 2016M601707, and Changzhou Sciences and Technology Program No. CJ20160016.

References

1. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
2. Koren, Y., Bell, R.: Advances in collaborative filtering. In: Ricci, F., Rokach, L., Shapira, B. (eds.) Recommender Systems Handbook, pp. 77–118. Springer, Boston, MA (2015). https://doi.org/10.1007/978-1-4899-7637-6_3
3. Yuan, W., Guan, D., Lee, Y.K., Lee, S., Hur, S.J.: Improved trust-aware recommender system using small-worldness of trust networks. Knowl.-Based Syst. **23**(3), 232–238 (2010)
4. Yuan, W., Guan, D.: Optimized trust-aware recommender system using genetic algorithm. Neural Netw. World **27**(1), 77 (2017)
5. Qi, L., et al.: Structural balance theory-based E-commerce recommendation over big rating data. IEEE Trans. Big Data (2016)
6. Han, G., Que, W., Jia, G., Shu, L.: An efficient virtual machine consolidation scheme for multimedia cloud computing. Sensors **16**(2), 246 (2016)
7. Han, G., Chao, J., Zhang, C., Shu, L., Li, Q.: The impacts of mobility models on DV-hop based localization in mobile wireless sensor networks. J. Netw. Comput. Appl. **42**, 70–79 (2014)
8. http://www.trustlet.org/epinions.html
9. Zhang, J., Lin, Y., Lin, M., Liu, J.: An effective collaborative filtering algorithm based on user preference clustering. Appl. Intell. **45**(2), 230–240 (2016)
10. Moradi, P., Ahmadian, S.: A reliability-based recommendation method to improve trust-aware recommender systems. Expert Syst. Appl. **42**(21), 7386–7398 (2015)
11. Lee, W.P., Ma, C.Y.: Enhancing collaborative recommendation performance by combining user preference and trust-distrust propagation in social networks. Knowl.-Based Syst. **106**, 125–134 (2016)