

Using Costumer Behavior to Build Social Network Based On Mole-Algorithm



Saba M. Hussain, Ghaidaa A. Al-Sultany

Abstract: The modern technology has great interrering on building relationships between users on social networking. Therefore, it is possible to promote goods, advertisements and rumors among people easily. A trust network is created for each member. With this model, Members are represented as nodes in the graph, and trust relationships are represented between members according to the directed edges. This approach is based on the premise the neighbors with higher trust ratings are likely to agree with each other about the trustworthiness. The question here is: how can trust networks be built between users? This work proposed to build a social network based on the Mole algorithm. The user's behavior is extracted to be use instead of user's rates in the original mole algorithm. The outcomes of this method were of a higher satisfactory level and a remarkably increased accuracy value by 15% over traditional Mole algorithm.

Keywords: Social Network, Mole Trust, Recommender System, Data mining.

I. INTRODUCTION

As the adaption of the internet increases, networked computer systems are playing a growing, vital role in our society. The expanding data and network technology lead to a rapid growth in the amount of information that has been generated through human activity. Therefore, "Information Overload" is becoming a serious issue [1]. A suggested solution to this problem could be using Recommender Systems (RSs). These systems aim to present suggestions of recommended products and services, as well as data that could be of the user's interest, taking their demands and preferences into consideration. Recently, RSs have increased in popularity, with applications in various domains. This indicates that a Recommender System could be an effective tool helping users find the item of interest and thereby present a solution to the issue of information overload [2]. Social context, on the other hand, is a much wider notion, as it does not only include the connections within social networks but also the different aspects of side data, like tags.

In addition, it could also be comprehended in a network-agnostic manner, being a distinct case of RSs with context-sensitivity [3]. The social setting leads to a set of human-centric factors like trust, which tends to play a significant role whenever users become aware of the participants' identity during the process of feedback. Social Trust, the type of trust that is found in web-based social networks, has several remarkable properties among which are trust transitivity, asymmetry, and personalization. It is proposed that trust transitivity differs from its mathematical sense in several ways. Trust asymmetry points out that the level of trust worth from user1 to user2 does not show similarity to its corresponding level from user2 to user1. For trust personalization, this characteristic suggests that it is merely a personal opinion [4]. Another aspect is user trust, which can be defined as the subjective prospect made by an entity about the future behavior of another. Such a trust network is constructed for each member. In this model, members are presented as nodes within the graph, whereas the direct edges show the level of trust among members. Trust algorithms have been used to support trust between authentic users. Trust-centric methods can be useful in the creation of robust RS. In order to corporate trust into the RS, trust propagation and aggregation methods are used with unsupervised methods, whereas supervised methods apply link predicting and the factorization of matrices for a performance of higher effectivity [5, 3]. In social networks, many algorithms are used in the computation of trust between users such as: Tidal, Modal, and Walk random algorithms, etc. Huge emphasis has been put on the algorithm used in computing peer-to-peer trust, some of which were adapted for social network environments. One of the attributes of using an application that collects users- and product data from a dataset is the extraction of certain features needed in the application of the algorithm itself. The drawback of this algorithm is using the rating only to compute trust between users. This work suggests a modification of the Mole algorithm for trust networks, using an algorithm to compute trust among users by using user behavior that will be obtained from dataset instead of rating within a given network. The detailed sections of the research paper are as follows.

Manuscript published on November 30, 2019.

* Correspondence Author

Saba M. Hussain*, University of Babylon, Department of Information Network, College of Information Technology, Babil, Iraq.

Ghaidaa A. Al-Sultany University of Babylon, Department of Information Network, College of Information Technology, Babil, Iraq.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Section 2 is described the related work . Section 3 deals with Moler trust algorithm. Section 4 explain how modify mole trust algorithm.

The dataset description in 5 and the result can see it in section 6 and the section 7 inducements conclusions and examines the possibilities of next future.

II. RELATED WORK

Some of the previous works in the same field have been reviewed within this section, such as:

Chuanmin Mi et.al.,(2018),[6] suggested a model of probability matrix factorization with the integration of social trust and the interests of the users. The model identified implicit trust relationships between users and labels of possible interest from the user's rating point of view. Another model of this type was used to carry out the matrix decomposition of the data of user rating, trust, and interest. Data sparseness is then eased through further determination of the user's characteristics. After that, an experimental procedure based on the dataset of Epinion's website is applied for the verification of the proposed method.

Hao Tian et. al., (2017),[7] suggested an enhanced method based on trust connections within social networks which aims to further develop the notion of recommending. Trust connection is particularly defined afresh, taking into account various representative factors with the interpretation of trust relationships. For a more comprehensive verification of the suggested approach, the experiments dealt with in this paper have been carried out in three different ways. The initial results of the experiments indicate that the suggested method results in a substantial extension in terms of the accuracy of prediction and is therefore of great use in approaching cold start and sparsity.

R. Logesh et. al., (2017)[8] presents a POI (Point-of-interest) recommendation method that is mainly based on the improvement of trust within social networks, also recognized as social pertinent trust walker (SPTW). A matrix factorization technique is used in calculating the amount of trust among users within such a social network. SPTW with an algorithm of relatively high probability location category contribute to the creation of POIs in form of recommendation lists.

Munmun and Nashreen (2016), [9] their paper shows an algorithm for the inference of trust propagation among individuals who are linked indirectly within a network, using weighted trust ratings which form the shortest as well as most dependable path. DIJKstar is used here to define the SPA. The reliability level for this algorithm in the prediction of propagated trust is measured and put into comparison with the simple average strategy as well as the multiplicative strategy algorithm. The latter has been tested on five actual trust datasets with the

attempt to identify the presence of a significant positive correlation between direct trust and the corresponding propagated trust collected throughout this method.

Partha(2012),[4] presented three designs for algorithms of trust propagation which are mainly based on the simplified multiplication strategy of trust propagation. Among the factors that are taken into account in calculating this propagated trust are the path length and the decay of direct trust values. The level of reliability of the algorithm in terms of the prediction of propagated trust values is determined and put into comparison with the Mole Trust algorithm. In order to evaluate the metric of measuring range propagated trust values taken form the divergence substantial trust rating, the Mean Absolute Error (MAE) has been used.

The aim of this work is to discover methods to use the social graph structure and the trust relationships between them to deduce the extent to which two individuals who share no direct connection might trust each other.

III. MOLETRUST ALGORITHM

Mole trust algorithm is one of the social network trust algorithms, a supervised method to build a trust network between users on internet and social media. This algorithm calculates trust from the first source to all other nodes within the maximum distancing range of two stages in advance. Since no source is specifically used in the, a varying standard (in terms of maximum path length δ) is applied to terminate the calculation of the shorter path [5]. In addition, the user-defined confidence threshold α is applied in all source pairs, rather than having one calculated for each source sink pair [3]. MoleTrust seems to have a relatively higher efficiency than other Trust algorithms, as it simply needs to be applied for each source node only once. In the termination of computing the shorter path, a different criterion (regarding maximum path length δ) has been used, for a sink does not have exact specification in Mole-Trust.

The Mole-Trust algorithm could be presented in two steps. The first step is the removal of the cycles within the trust network whereby it is transformed into a directed acyclic graph. The second steps involves a graph walk that starts from the source node and aims to calculate trust score of the nodes that have been visited An example below (Figure 1) shows the prediction of the trust score of user X towards Z. The Mole-Trust only allows the rating of A and B about X, and thereby declines the trust statement made by C, as the predicted trust score of C is 0.1, lower than the (0.5) threshold used in this example. Consequently, the predicted trust score of Z equals $(0.8 \times 0.6 + 0.9 \times 1.0) / (0.7 + 0.9) = 0.825$.

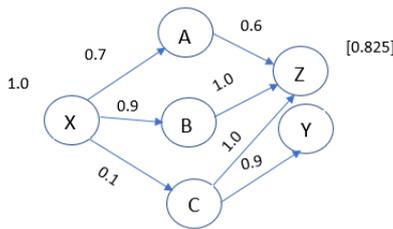


Figure 1: An example for Mole

The formula (1) of the predicted score of a user is as follows:

$$trust(u) = \frac{\sum_{i \in \text{predecessor}(trust(i) * trust_edge(i,u))} (1)}{\sum_{i \in \text{predecessor}(trust(i))} (1)}$$

Then the rating deviation is used as a weight for the links between users, from which the trust between users can be calculated in algorithm 1:

Algorithm1

- 1: Set Mole algorithm parameters
- 2: User rating score [] ← Extract From dataset
- 3: for user I ← to all users find
- 4: $user_{rating}(i) \leftarrow \frac{\sum_{ij=1}^n \sum User\ rating}{n}$
- 5: for user I ← to all users find
- 6: Social Net (User i) ← []
- 7: for user j ← All users
- 8: if user I & user j shard product
- 9: $Trust(u) \leftarrow \frac{\sum(trust(i) * trust_edge(i,u))}{\sum trust(i)}$
- 10: if trust (u) > .5 then
- 11: user I trust User j
- 12: Social Net (User i) ← Social Net (User i) ∪ User j
- 13: Return Social Network
- 14: End

An algorithm1: Traditional mole trust algorithm

IV. MODIFY WEIGHT OF MOLE TRUST ALGORITHM

This section discusses the mole trust algorithm after being enhanced, such as the adjustment of the weight used by replacing it with the value of the spam score that resulted from extracting some features from a dataset about users and products. Some features are imported from a dataset, such as the username and product ID whereas other features are extracted from the same dataset like the similarity of text (each user review on the products), fairness for users, number of reviews per product (NRP) and goodness. Apart from all features will be the analysis of the user’s behavior history and the combination of (Sim, NRP and Fairness) in one equation, called spam score [10]. The following table (1) explains the main equation that will be used to calculate user's behavior in the spam score:

Table 1

Explain the main equation that using in proposed system [11]

SQ.	Feature name	Range	Value Prefer	
			Authentic	Fake
1	NRP:	[0,1]	Small	High
	$NRP_i = \frac{Hista,j}{na,p}$			
2	Fairness:	[0,1]	Small	High

$$Fairness_i = \frac{\sum_{j=1}^n \dot{R} - \sum_{j=1}^m}{\sum_{j=1}^n R}$$

SIM:

$$Sim_i = T F t \times d \log \left(\frac{N}{D F t} \right) \quad [0,1] \quad \text{Small} \quad \text{High}$$

Goodness:

$$D = \Delta g - \Delta b$$

$$g = \frac{(U_g + 1)}{((T_r - D) + 1)}$$

$$b = \frac{(U_b + 1)}{((T_r - D) + 1)} G($$

$$= \begin{cases} 0 & g > b \\ 1 & otherwise \end{cases}$$

Two classes will be obtained from the spam score results to identify the user authenticity of users. In order to create social network trust, new weight between the users (spamscore) extracted from user behavior will be applied [11].

The following formula (2) shows how the results of the spam score are calculated:

$$SpamScore_i = \frac{\sum_{i=1}^n (Fairness_i + NRP_i + sim_i)}{3} \quad (2)$$

After calculating the spam score for user, the system will classify the user as in the equation 3:

$$User_{typei} = \begin{cases} fake & \text{if } Spam\ Score_i > \alpha \\ Authentic & \text{otherwise} \end{cases} \quad (3)$$

It is noticed that the trust between users starts to form larger aggregates or clusters, as each group the users are either all authentic or non-authentic, depending on their classification. Therefore, it appears that there is no problem unless the group is a hybrid. In this case, the non-authentic will be excluded if the dominate category is authentic, and vice versa. Afterwards, the groups are compiled correctly and their integration has been worked on to obtain totals as the largest number of users with trust among them. Below is shown the algorithm (2) of Mole Trust after modification: -

Algorithm2

- 1: N : number of user features
- 2: Set Mole algorithm parameters
- 3: ser behavior score[] ← Extract n feature as user behavior
- 4: for user I ← to all users find
- 5: $user_{Userbehavior\ score}(i) \leftarrow \frac{\sum_{ij=1}^n \sum User\ behavior_j}{n}$
- 6: for user I ← to all users find
- 7: Social Net (User i) ← []
- 8: for user j ← All users
- 9: if user I & user j shard product
- 10: $Trust(u) \leftarrow \frac{\sum(trust(i) * trust_edge(i,u))}{\sum trust(i)}$
- 11: if trust (u) > .5 then
- 12: user I trust User j
- 13: Social Net (User i) ← Social Net (User i) ∪ User j
- 14: Return Social Network
- 15: End

An algorithm 2: modify mole trust algorithm

V. DATASET DESCRIPTION

Reviews from amazon.com [12] are used which represent one of the most successful online e-commerce sites with a long and reliable history. The reason behind using this dataset is that they are cover a very wide range of products. In this work, two main categories of dataset (movie) are used. Each review in the amazon.com dataset consists of 9 attributes:

"<Reviewer ID><Asin><Rating><Date><Review Text><Reviewer Name><Helpful ><summary><Unix review time>".

Figure 2 shows the social network between users according to shared products.

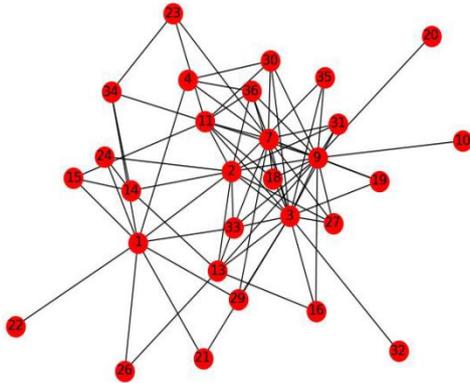


Figure 2: Sample Social network based on shared for 37uses.

VI. THE RESULTS AND DISCUSSION

This section of the research discusses the results obtained from the algorithm above,as well as the results of improving the algorithm and comparing them to find out the usefulness of improvement in building a trust network between users on the Internet.

A. Experiment Result of Mole Trust Algorithm:

Mole algorithm is considered to be the most convenient to use as its principle depends on the traffic of the contract once, taking the largest path in terms of weight as the approved rating given by the user on the product. The results were positive as the work accuracy was about 45%. Figure (3) below explains the result of the Mole Trust:

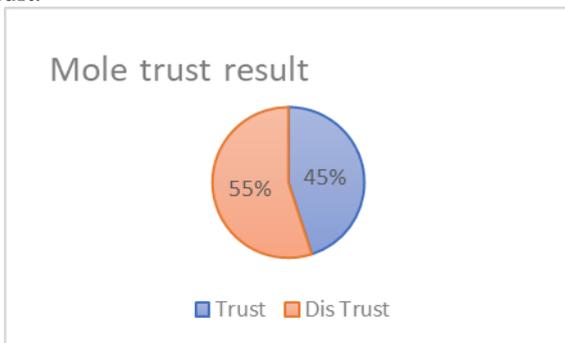


Figure 3: Mole Trust Network Result

Figure 4 illustrate the trust social network for 200 records (37 users) of amazon dataset that mentioned in [12] by using mole trust algorithm.



Figure 4: mole trust social network for 37 users

B. Experiment Result of Modify Mole Trust Algorithm:

This algorithm has been improved to find the largest number of users among them, based on adjusting the weight used by replacing it with the value of the spam score that resulted from the classification mentioned above. It is noticed that the trust between users starts to form larger aggregates or clusters, as each group the users are either all authentic or non-authentic, depending on their classification. Therefore, it appears that there is no problem unless the group is a hybrid. In this case, the non-authentic will be excluded if the dominate category is authentic, and vice versa. Afterwards, the groups are compiled correctly and their integration has been worked on to obtain totals as the largest number of users with trust among them. By applying the updates aforementioned, it has been noticed that the accuracy ratio equaled about 60% for the same data that was selected. Figure (5) below explains the result after modifying the mole trust algorithm

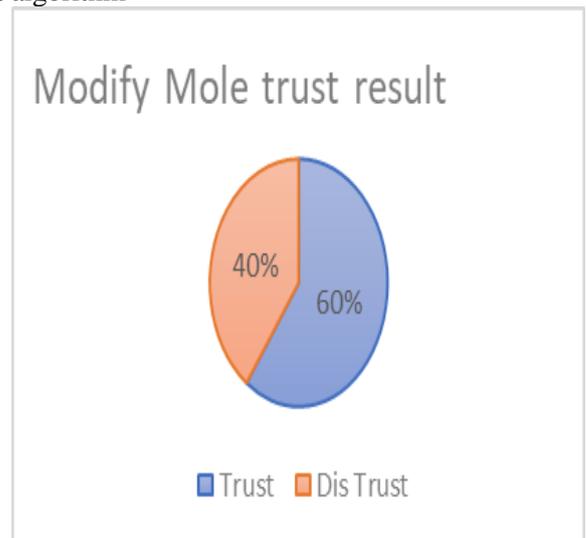


Figure 5: Modify Mole Trust Algorithm

After using the spam score as weight instead of rate in mole trust Mole Network the size of trust network is increasing. Figure 6 illustrate the trust social network for 200 record of amazon dataset [12]

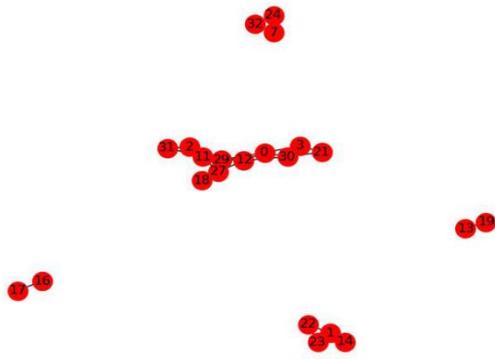


Figure 6: mole trust social network for 37 users

Finally, looking all previous results we can say that our algorithm succeeds in build biggest trust network between users. This demonstrates that use spam score for mole trust algorithm as weight is best for building trust relation between users.

VII. CONCLUSION

Social networks provide an important source of information about users and their interactions. This forms a special value in recommendation systems. This work proposes a Social Network Recommendation system (SNRS) based on a social network that creates recommendations by looking at the user's own preferences, general acceptance of the element and its impact from friends. This social network is built based on the Mole algorithm. The user's behavior is extracted to use instead of user rates in original mole algorithm. The drawback of this algorithm is using the rating only to compute trust between users. Rating only doesn't give a sufficient impression of the person as a weight between users. Therefore, in this work applied traditional mole algorithm and will be modifying it by using the result of spam score as a weight between users. This method is considered to be of a relatively higher satisfaction regarding the results, as the outcomes of the mentioned algorithm had a higher accuracy. The results were acceptable using the algorithm, yet after adjustment the results seemed to be much more satisfactory and had a higher level of accuracy. The accuracy of the system, for instance, equaled about 45% before modification, and reached a percentage of 60% afterwards.

REFERENCES

1. Chuanmin Mi and et. al, 2018, "A Recommendation Algorithm Considering User Trust and Interest", Springer International Publishing AG, part of Springer Nature.
2. Faezeh Sadat Gohari and et. al., 2017, "A semantic-enhanced trust-based recommender system using ant colony optimization", Springer Science+Business Media New York 2016, Appl Intell (2017) 46:328–364.
3. Charu C. Aggarwal, (2016), "Recommender Systems: text book", IBM T.J. Watson Research Center, Yorktown Heights, NY, USA.
4. ParthaSarathi Chakraborty, 2012 , "Designing trust propagation algorithms based on simple multiplicative strategy for Social

5. Networks", 2nd International Conference on Communication, Computing & Security [ICCCS-].
6. MirjamŠitum, , 2014, " Analysis of Algorithms for Determining Trust Among Freinds on Social Networks" , Faculty of Electrical Engineering and Computing, Vienna, June.
7. Chuanmin Mi et.al., 2018 ,"A Recommendation Algorithm Considering User Trust and Interest" , Springer International Publishing AG, part of Springer Nature.
8. Hao Tian et.al., 2017, " Improved Recommendations Based on Trust Relationships in Social Networks", Future Internet, 9, 9; doi:10.3390/fi9010009m.
9. R. Logesh et.al., 2017, "A Reliable Point of Interest Recommendation based on Trust Relevancy between Users", Published online: 29 June 2017 _ Springer Science-Business Media, LLC.
10. Munmun Bhattacharya et.al., 2016, "An Algorithm for Predicting Local Trust based on Trust Propagation in Online Social Networks", International Journal of Computer Applications (0975 – 8887) Volume 156 – No 7, December.
11. Ghaidaa A. Al-Sultany and Saba Mohammed Hussain, 2019," User Behaviour Analysis for the Merchandises Fairness Evaluation", International Journal of Engineering & Technology, 8 (1.5) (2019) 138-143.
12. Ghaidaa A. Al-Sultany and Saba Mohammed Hussain, 2019," Fake reviews detection through users behavior analysis". <http://jmcauley.ucsd.edu/data/amazon>, 2018.

AUTHORS PROFILE



Saba Mohammed Hussain is completed B.Sc. in Computer Sciences in 1998 from the college of sciences at University of Babylon, Babil, Iraq. Received his M.Sc. (master) in computer sciences in the year 2011 from the college of computer sciences at the Babylon University (BU), Babil,Iraq.She has worked as a lecturer in Information Technology in Babylon Universities in the areas of Artificial Intelligent, Information System and Data base. she currently works as a lecturer in the University of Babylon in information Technology. Her research interests machine learning, social network algorithms.



Gaidaa A. Al-Sultany had her PHD in semantic computing and data mining from Brunel University , UK(2012). She's currently working a professor in Information Technology College, University of Babylon, Iraq. Her research area focuses on text Analysis and Social networks relationships. She published more than 30 research paper.