Applied and Computational Mathematics
2017; 6(4): 208-214
http://www.sciencepublishinggroup.com/j/acm
doi: 10.11648/j.acm.20170604.19
ISSN: 2328-5605 (Print); ISSN: 2328-5613 (Online)

Credibility Evaluation Algorithm Based on Deep Learning

Liu Mengling[1, *], Li Zhendong[2]

[1]Department of Mathematical Sciences, Tsinghua University, Beijing, China
[2]School of Information and Control, Nanjing University of Information Science & Technology, Nanjing, China

Email address:
evelyn1219@163.com (Liu Mengling)
[*]Corresponding author

To cite this article:
Liu Mengling, Li Zhendong. Credibility Evaluation Algorithm Based on Deep Learning. *Applied and Computational Mathematics*. Vol. 6, No. 4, 2017, pp. 208-214. doi: 10.11648/j.acm.20170604.19

Received: July 1, 2017; **Accepted**: August 5, 2017; **Published**: August 17, 2017

Abstract: The credibility of a recommendation system is a hot focus nowadays in the field of personalized recommendation research. However, it is difficult to carry out effective credibility evaluation for the users in the presence of a false recommendation system, say nothing of eliminating suspicious users and further more improve the security and reliability of the system. This paper proposed a new method of reliability assessment based on deep learning. According to the users' rating database, community of users with average scores is constructed and traditional credibility algorithm is used to calculate the initial credibility of the users. With the average users' reliability value as a criterion, the second assessment to the credibility based on deep learning algorithm is applied to other users, the results of which are arranged in ascending order. Then suspicious users ranking *top-L* will be removed and a trustfully adjacent group for the target users will be created. Experiments show that the improved algorithm can optimize the recommendation system with better security, accuracy and reliability as well.

Keywords: Reliability, Average User, Deep Learning, Accuracy

1. Introduction

With the rapid development of information technology and the advent of the "big data" era, the openness and interactivity of the recommendation system make the false score-data more possible to be injected. In the personalized recommendation system, if you want to provide accurate prediction and recommendation for the target users, the authenticity of the users' information and the reliability of the system are rather essential. For commercial competition and somewhat other purposes, some network users input a large number of false evaluation and scores into the recommendation system, so that the recommendation system will produce favorable results for them to increase their business interests. The consequences of all these are concern attacks on the recommendation system, resulting in a decrease in the credibility of the recommended system and affecting the final decision of the target users.

After the academic status of mass-communication was established in 1950s, the credibility research has become the focus of many scholars. First, the credibility research was only aimed at the disseminators, which called information-source credibility. With the development of science and technology, the media is also developing from newspapers and television to today's Internet. So the credibility research is also changing to focus on Internet e-commerce. Without doubt, the study of the recommendation credibility is a hot research topic in the "big data" era, and its concentration is also transferred from the original study to the credibility of the media to the later study to credibility of the recommendation system. In 2013, Qin Jiwei and others proposed that when we search neighbors for the target users, the credibility should be defined as the deviation between the target user's recommendation scores and the system's average value, and the high weight should be given to the evaluation scores of the user with higher credibility [1]. In 2014, Liu Shengzong and others proposed a new recommendation algorithm taking both the users' credibility and similarity into account. They analyzed the three main credibility factors, such as the adoption rate of the users' evaluation, the correctness of the scores and the number of scoring, and then established the relationship between the credibility and the three factors [2]. In experiments, they found that attacking users' filling in the scoring matrix is obviously more than others, so the number of scoring will also be more. If scoring number $n_x > H$ (the threshold value) still be considered as one of the factors in credibility evaluation, it will be unreasonable, and the user's rating accuracy will be affected, then affect the entire credibility assessment system, resulting in the effectiveness decrease of recommendation accuracy. And when calculating the credibility, if a researcher only concentrate on the user's scoring data, which is just a vertical comparison, and pay no attention to horizontal comparison, such as comparing with other users or users with high credibility, such an analysis must have limitations on assessment of users' credibility and cannot evaluate effectively all around.

In this paper, we'll propose a new algorithm of reliability assessment based on deep learning. According to the users' rating database, we first construct the initial credibility matrix of users and the users with average scores as a benchmark, while apply deep learning algorithm for the second assessment of the credibility to other users, the results of which are arranged in ascending order, then suspicious users ranking *top-L* will be removed for the target users. Experiments show that the improved algorithm can raise both the security and accuracy of the recommendation system to a certain extent.

2. Introduction to the Recommendation System

Due to the openness of the evaluation of the recommended system in e-commerce platform, some network merchants (commonly known as attackers) will add false rating into the system in order to increase their interests or to discredit their opponents, which seriously undermine the recommendation fairness.

Table 1. *Scoring matrix with attacking users.*

	i_1	i_2	i_3	i_4	i_5	i_6
A	5	1	3	3		4
B	5		3	2		
C	5	3		3	3	
D					5	
E	2		4		4	
*att*1	1	1	1	5	1	4
*att*2	5	1	5	1	1	1
*att*3	5	5	1	4	1	5

According to the attacking means, attacks above can be classified as two categories, named as push attack (the scoring to i_1 by att2 and att3, aiming at increasing the scores.) and nuke attack (the scoring to i_5 by att1, att2 and att3, aiming at decreasing the scores.). Based on different models, the attack profile can also be divided into four parts, including the target item, filling item, selected filling item and no rating item. Random attack, average attack and bandwagon attack are three typical attack models [3].

3. Relevant Study on Credibility Algorithm

It is because the attacking data existing in recommendation system, the reliability of users declines and the precision of recommendation goes down too. So, we should exclude the attacking users and find the reliable users for target users. This part will give a detailed introduction to the relative credibility algorithm as follows:

3.1. Credibility Algorithm for Users

Traditional credibility algorithm determine the credibility of users by their numbers of scoring and the scoring accuracy which estimated by score comparison. As shows in Table 2.

Table 2. *Credibility matrix for users.*

	Item1	***Item2***	**...**	***ItemJ***	**...**	***ItemN***	T_u
User1	E_{11}	E_{12}	...	E_{1J}	...	E_{1N}	T_{u1}
User2	E_{21}	E_{22}	...	E_{2J}	...	E_{2N}	T_{u2}
...	...	...	...	...	...	...	
UserI	E_{I1}	E_{I2}	...	E_{IJ}	...	E_{IN}	T_{uI}
...	...	...	...	...	...	...	
UserM	E_{M1}	E_{M2}	...	E_{MJ}	...	E_{MN}	T_{uM}

The reliability of a user is determined by two factors, named as the number of scoring and the score accuracy of the users.

3.1.1. The Number of Scoring

The scoring number of a user can be used as a measurement to his vitality and also an important factor when estimating his scoring credibility. Here, the weight of the scoring number can be defined by:

$$w_{\mathrm{u}} = \begin{cases} 1 & n_x \geq H \\ n_x / H & n_x < H \end{cases} \tag{1}$$

w_u means when the scoring number $n_x \geq H$, then the credibility of the user is higher (H is an adjustable parameter, experiments in subsequent parts will illustrate that when it reaches 1/9 of the items value, the effectiveness will be the best.).

3.1.2. The Accuracy of Scoring

In daily shopping, customers always refer to other people's advice when buying goods, or the average level of the item he buys. So, the scoring accuracy is commonly measured by the mean value of the scores which are given by clients who buy the item.

$$E_{u,i} = 1 - \frac{\left|R_{u,i} - \overline{R_i}\right|}{S} \tag{2}$$

Where, $E_{u,i}$ is the scoring accuracy of Client u for Item i, $\overline{R_i}$ is the average score for Item i, S is the maximum rating for Item i by Client u.

3.1.3. The Client Credibility

Integrating the scoring number and the scoring accuracy to decide the client credibility:

$$T_u = w_u \times \frac{\sum_{i=1}^{n} E_{u,i}}{n} \tag{3}$$

Where T_u means the reliability of Client u, n means the quantity of items.

The definition above denotes that the credibility is a statistic value which is used to represent the reliability of the rating scores given by the client.

3.2. Analysis to the Algorithm Mentioned Above

The algorithm mentioned above has some shortages when the scoring data is attacked by some clients:

(1) According to previous introduction of attacking, the compactedness of the attacking client to scoring matrix is high when he makes attack to scoring data, which means his scoring number will also be high. That is to say, $n_x \geq H$ will not be used as a factor to evaluate the credibility of a client any longer because it will affect w_{u_i} and further the overall credibility estimation system, which decreases the accuracy of the recommendation system as a result.

Described in the dataset presented in Table 2, if client u_5 is put in as an attacking client in the scoring matrix, the fact is that the scores given by client u_5 is almost opposite to the other 4 clients. According to the credibility algorithm above, scoring number of client u_5 reaches the request and is selected to be reliable, this is weird and irrational.

Table 3. *Data set.*

	i_1	i_2	i_3	i_4	i_5	i_6	i_7
u_1	1	2	3		4	5	1
u_2	2	3	3	1	5	4	2
u_3	1	3	3	1	4	5	1
u_4	2	2	3		3	4	1
u_5	5	5	1	4	1	2	5

In the credibility matrix showed in Table 4, generally the reliability of client u_5 will be the lowest, but according to the results calculated by the algorithm above, a normal client u_3 has the lowest reliability, this is irregular and the shortage is obvious.

Table 4. *Credibility matrix.*

	i_1	i_2	i_3	i_4	i_5	i_6	i_7	T_u
u_1	31/25	6/5	23/25		22/25	4/5	6/5	0.891
u_2	26/25	1	23/25	26/25	17/25	1	1	0.954
u_3	31/25	1	13/25	26/25	22/25	4/5	6/5	0.840
u_4	21/20	5/4	18/20		22/20	1	5/4	0.936
u_5	11/25	3/5	33/25	11/25	37/25	7/5	2/5	0.880

(2) Based on the analysis to the algorithm above, it can be found that when evaluating the credibility of clients, if we only take the rating scores into account and make longitudinal comparison without a transversal one, the result will have its limitation and cannot estimate a correct credibility all around.

3.3. Improvement Ways

(1) Creates average clients u_{ave}, whose rating for each item is the average $\overline{R_i}$ obtained by excluding the highest and the lowest score for the item, and then take it as a criterion to make horizontal comparison with other guests.

(2) On base of calculating the credibility matrix for each client, apply deep learning algorithm to assess the credibility of each client for the second time, and estimate the similarity between average client and other clients to exclude all the clients with lower reliability, and finally establish a health neighbor group for target client.

4. The Improved Credibility Algorithm Based on Deep Learning

When the users wants to attack the recommendation system, he hopes to achieve the desired effect after filling the data as soon as possible, so his attack data will be very intensive, it is not feasible to use a traditional method to evaluate users' reliability. In view of the above conditions, with the average users' reliability value as a benchmark, we use the deep learning algorithm to compare the scores with the other users, and then get the order of users' reliability.

4.1. Construct Average Users

In our daily life, the average score represents the average level of a thing. This is also true in the recommendation system. In addition to the reliability assessment algorithm, the average score also plays a key role in most common attack detection algorithms. Generally we find the attack users by the average value of the item after determining the attacking time.

The paper proposes to establish average user u_{ave}, after removing the highest and lowest score, we use the rest to calculate the average score of each Item i. Assuming the degree of Item i is k_i, then each item's average score is:

$$\overline{R_i}^* = \frac{\sum_{m=1}^{k_i-2} r_{u_m,i}}{k_i - 2} \tag{4}$$

Regarding the average $\overline{R_i}^*$ of each Item i as the score of the average user u_{ave}, and adding it to the scoring matrix as a new user, then use the algorithm above to calculate the average users' credibility as a comparison criteria.

4.2. Deep Learning Algorithm

Using the two-layer Boltzmann machine in the recommendation algorithm has been studied in some foreign countries. In reference [4], the two-layer Restricted Boltzmann Machine has been modified into a Softmax model with the visible layer as the input layer and the hidden layer is a binary model. Generally, Softmax model is applied to represent discrete data structure, and only one row of each column is 1, all the rest are zeros. Referred in Figure 1, the block covered by grey is the effective row of each column.

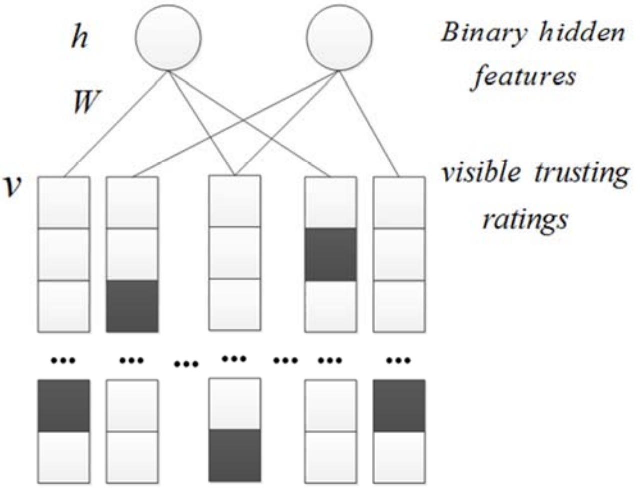

Figure 1. *Softmax structure.*

Suppose there are N users in the recommendation system. We use the credibility algorithm to calculate and establish the $N*1$ credibility matrix, which is transformed into a $K*N$ Softmax model. In experiments, we found that the credibility value is within the range of 0 to 1.

In order for convenience, the statistic data could be refined. If the credibility value is within the range of 0 to 0.01, we give K a value of 1, if within the range of 0.01 to 0.02, we give K a value of 2, and so on, the maximum of K is 100. The concrete structure is shown in Figure 1, where, the gray part has K rows, representing the magnitude of the user's traditional credibility.

Assuming $K = 100$ in the graph, which means the model has 100 rows and the input unit has 100 Softmax for each column, the model can be represented by a matrix V of $\mathrm{K \times N}$.

Assuming user u_i has the credibility K, the valuable on Row k and Column i in the Matrix can be represented by v_i^k. When $v_i^k = 1$, the credibility of the user is K. Let the hidden layer is h_j, $j = 1,...,F$, F is the number of hidden layers and the hidden layer is $\{0,1\}$. From the structure diagram, we can see that this model which contains the Softmax Boltzmann machine has a total of $N*F*K$ parameters needing adjusted. The Energy function of the model is:

$$E(V,h) = -\sum_{i=1}^{N}\sum_{j=1}^{F}\sum_{k=1}^{K} v_i^k h_j w_{ij}^k + \sum_{i=1}^{N} \log Z_i \tag{5}$$

$$Z_i = \sum_{l=1}^{K} \exp\left(\sum_{j=1}^{F} h_j w_{ij}^l\right) \tag{6}$$

Based on Eq. (5) and Eq. (6), when the state of visible units is given, the activation probability of hidden units is:

$$\begin{aligned} \hat{p}_j &= P\left(h_j = 1 \middle| v\right) \\ &= sigmoid\left(\sum_{i=1}^{N}\sum_{k=1}^{K} v_i^k w_{ij}^k\right) \\ &= \frac{1}{1+\exp\left(-\sum_{i=1}^{N}\sum_{k=1}^{K} v_i^k w_{ij}^k\right)} \end{aligned} \tag{7}$$

When the state of hidden units is given, the activation probability of visible units is:

$$P\left(v_i^k = 1 \middle| \hat{p}_j\right) = \frac{\exp\left(\sum_{j=1}^{F} \hat{p}_j\, w_{ij}^l\right)}{\sum_{l=1}^{K} \exp\left(\sum_{j=1}^{F} \hat{p}_j\, w_{ij}^l\right)} \tag{8}$$

If regard the average users' credibility as a standard, then assess the other users' credibility once again, finally select the recommended reliable users to target users. Therefore, when the training is over and the users' original credibility matrix is known as V, the probability evaluation with credibility K of the average users to user i can be found by Eq. (8).

The second credibility evaluation $\hat{r}$ of the average users to user i is:

$$\hat{r} = E\left[v_i\right] = \sum_{k=1}^{K} kP\left(v_i^k = 1 \middle| h\right) \tag{9}$$

Then we arrange $\hat{r}$ in ascending order and remove the suspicious users ranking $top - L$, calculate the similarity between the remaining users and the targets users and continuously complete the subsequent recommendation procedure.

4.3. The Relation of Restricted Boltzmann Machine and Algorithm of Selecting Trustful User Group

When RBM training is completed, we can estimate the user's credibility value by calculating the expectations defined in Eq. (9). However, in order to achieve the average user's recommendation on the trustfully adjacent group, it may be necessary to estimate the credibility of multiple users in the same time, that is to say, we need to calculate the following probability:

$$P\left(v_{q_1}^{k_1}=1, v_{q_2}^{k_2}=1, \ldots, v_{q_n}^{k_n}=1 \middle| V\right) \qquad (10)$$

With the growth of n, calculating Eq. (10) will be more and more difficult. So, Salakhutdinov [4] and others proposed a new method to calculate Eq. (10) approximately by using the Mean Field [5]. Now we introduce the Mean Field approximation method and its relation with the algorithm of selecting trustful user group.

Given the traditional credibility V to a user, use Eq. (7) to calculate the activation probability of the hidden units, then use the mathematical expectation of the activation probability of the hidden units to calculate the activation probability of all the visible units. So the activation probabilities of these visible units can be used as estimation of probabilities of the average users to the credibility of the remaining users in the recommendation system. Detailed calculation algorithm is in Eq. (7) and Eq. (8). It should be noted that because the hidden units only have two values, so:

$$E\left(P\left(h_j=1 \middle| V\right)\right)=0 \cdot P\left(h_j=0 \middle| V\right)+1 \cdot P\left(h_j=1 \middle| V\right)=P\left(h_j=1 \middle| V\right)$$

Eq. (11) is actually calculating the similarity between the user and the average user at the hidden layer based on RBM learning.

RBM is actually determined by the features of the hidden unit (the connecting weight from hidden units to all visible units). The purpose of training RBM is to find a set of features. Only when the training data have the maximum likelihood, they can be truly expressed by these features. In this context, these features can be understood as average users who can represent the user's credibility, which is represented by hidden unit j.

Given a credibility V to some users, then according to Eq (7), the activation probability of the hidden units can be calculated by two steps as follows: first, find the transvection of the two matrices: V and $w_{\cdot j}$ of the hidden units (i.e. the similarity between common users and average users); second, apply Sigmoid function to compress it within the range of $[0,1]$. Assuming the credibility of user u_i is k (i.e. $v_i^k=1$), and if w_{ij}^k is more, then the transvection will be more, which means the activation probability of the average user (represented by j) also will be more. The Sigmoid is a monotonic increasing function.

So, to some extent, the activation probability of the hidden unit j can be regarded as the degree of conformity (similarity) of the credibility V of a certain user to the credibility of the average user represented by the hidden unit j.

Based on the above discussion, if we regard $\hat{p}_j$ as the similarity between the user V and the average user j, then it can be found that the second evaluation of the user's credibility is directionally proportional to the linear combination of the average user who is similar to him:

$$P\left(\hat{V} \middle| \hat{p}\right) \propto \exp\left(\sum_{j=1}^{F} \hat{p}_j w_{\cdot j}\right) \qquad (11)$$

The activation probability of the hidden units corresponds to the similarity between the credibility of other users and the average users. And the average users correspond to the original users learned by RBM. Thus we have initially established the link between RBM and the reliability evaluation. First, based on CD algorithm, RBM can learn the features which may represent the credibility of the training set to the maximum extent. Then, estimate the users' credibility secondly according to the calculation result of traditional credibility algorithm.

4.4. The Relation of Restricted Boltzmann Machine and Algorithm of Selecting Trustful User Group

The algorithm flow chat is as Figure 2 shown:

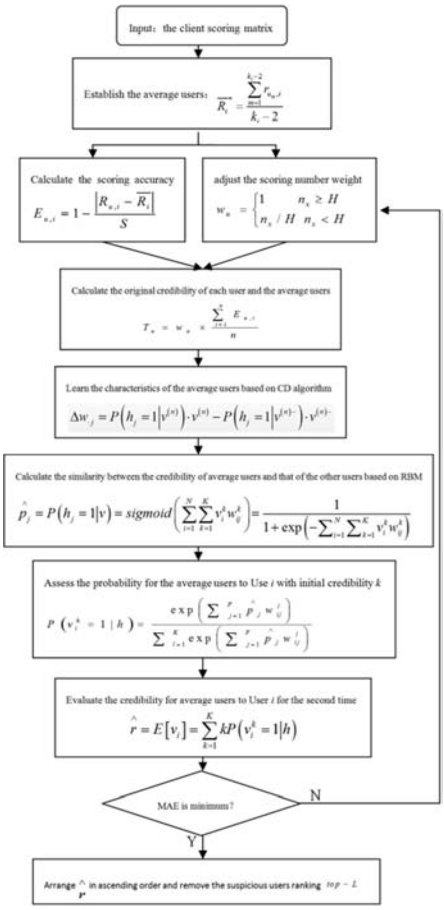
Input: the client scoring matrix
Establish the average users: $\overline{R_i} = \frac{\sum_{m=1}^{k_i-2} r_{u_m,i}}{k_i-2}$
Calculate the scoring accuracy $E_{u,i} = 1 - \frac{\left|R_{u,i} - \overline{R_i}\right|}{S}$
adjust the scoring number weight $w_u = \begin{cases}1 & n_u \geq H \\ n_u / H & n_u < H\end{cases}$
Calculate the original credibility of each user and the average users $T_u = w_u \times \frac{\sum_{i=1}^{n} E_{u,i}}{n}$
Learn the characteristics of the average users based on CD algorithm $\Delta w_{ij} = P\left(h_j=1 \middle| v^{(n)}\right) \cdot v^{(n)} - P\left(h_j=1 \middle| v^{(n)-}\right) \cdot v^{(n)-}$
Calculate the similarity between the credibility of average users and that of the other users based on RBM $\hat{p}_j = P\left(h_j=1 \middle| v\right) = sigmoid\left(\sum_{i=1}^{N}\sum_{k=1}^{K} v_i^k w_{ij}^k\right) = \frac{1}{1+\exp\left(-\sum_{i=1}^{N}\sum_{k=1}^{K} v_i^k w_{ij}^k\right)}$
Assess the probability for the average users to Use *i* with initial credibility *k* $P\left(v_i^k = 1 \mid h\right) = \frac{\exp\left(\sum_{j=1}^{F} \hat{p}_j w_{ij}^k\right)}{\sum_{l=1}^{K} \exp\left(\sum_{j=1}^{F} \hat{p}_j w_{ij}^l\right)}$
Evaluate the credibility for average users to User *i* for the second time $\hat{r} = E\left[v_i\right] = \sum_{k=1}^{K} kP\left(v_i^k = 1 \middle| h\right)$
MAE is minimum?
N
Y
Arrange $\hat{r}$ in ascending order and remove the suspicious users ranking top − L

Figure 2. *The flow chart.*

4.5. The Comparison of some Credibility Algorithms

Three other credibility algorithms are selected to compare with the improved algorithm proposed in this paper, which named as: BN [6], TCF [7], SRP-CCF [2]. The algorithm accuracy is denoted in Figure 3 and Figure 4.

As the definition says, the smaller the value of MAE and RMSE, the better the recommendation accuracy. As can be seen from Figure 5 and Figure 6, the red curve represents the improved algorithm in this paper. Let the number of the nearest adjacent group K go from 10 to 50, the MAE and RMSE of the improved algorithm proposed by this paper are always lower than the algorithms that other scholars proposed, which shows that the improved algorithm accuracy is better to some extent.

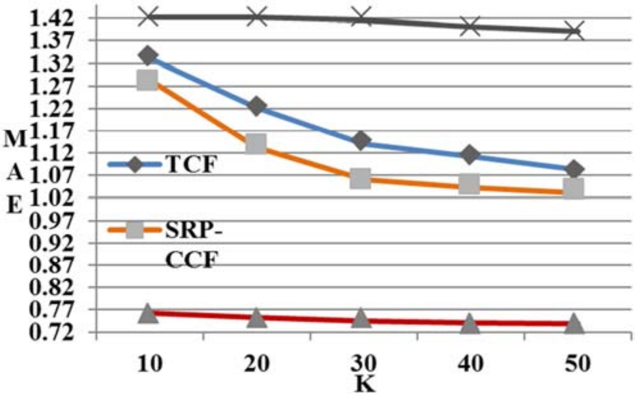

Figure 3. *MAE comparison.*

As shown in Figure 3, the abscissa axis is marked as the nearest adjacent number K and the ordinate is for the value of MAE. K increases from 10 to 50, and the interval is 10. With the increase of K, MAE is being reduced, and finally intend to be stable, which shows that the nearest adjacent number affects the recommended accuracy.

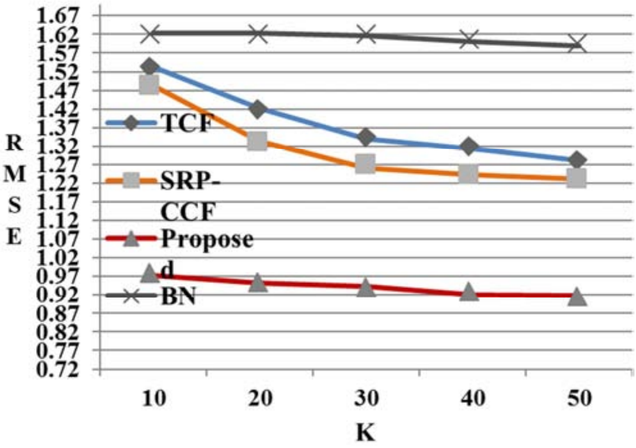

Figure 4. *RMSE comparison.*

As shown in Figure 4, with the increase of K, the RMSE of the algorithm proposed in this paper is always lower than other algorithms, which shows that the improved algorithm accuracy is better than others. The abscissa axis is marked as the nearest adjacent number K, and the ordinate is for the value of RMSE. K increases from 10 to 50, and the interval is 10. With the increase of K, RMSE is being reduced, and finally intend to be stable, which also shows that the nearest adjacent number affects the recommended accuracy.

4.6. The Effect of the Threshold Selection of the Evaluation Number

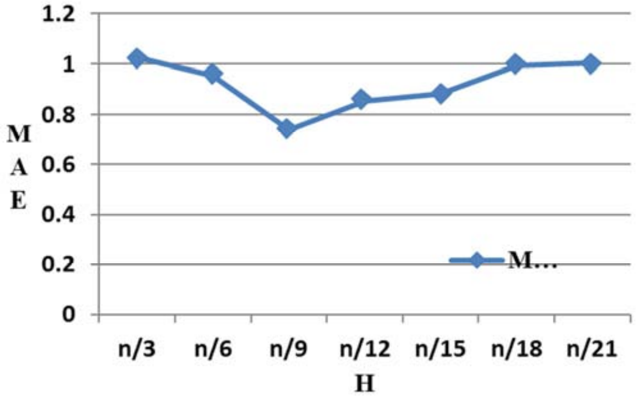

Figure 5. *The effect of the threshold selection of the evaluation number.*

As shown in Figure 5, the abscissa axis is for the threshold H of the evaluation number, and n is the number of items. It can be found that when the threshold is $n/9$, the value of MAE is the smallest and the precision is the highest.

4.7. The Effect to the Recommendation Accuracy by Removing the Suspicious L Users

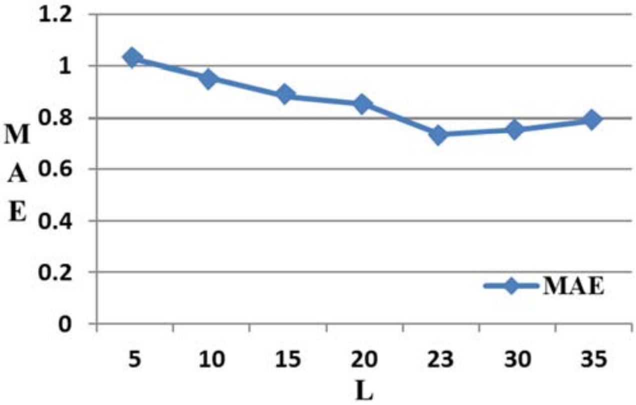

Figure 6. *The effect to the recommendation accuracy by removing the suspicious L users.*

As shown in Figure 6, after the second assessment of the credibility and arranging in ascending order, suspicious users ranking $top-L$ will be removed. In the experiment, it is found that when L is 23, the MAE is the smallest, and the recommendation accuracy is the best.

5. Conclusion

The users' credibility assessment is a very important research topic in the security and reliability of a personalized recommendation system. When the evaluation matrix (also denoted as scoring matrix) is maliciously attacked, the traditional credibility algorithm can not accurately assess the users' credibility. This paper proposes a new algorithm, with the average users' reliability value as a criterion and based on deep learning, a second assessment of the credibility is applied to other users, the results of which are arranged in ascending order. Then suspicious users ranking $top-L$ will be removed and a trustful adjacent group for target users will be created. The later experiments show that the accuracy of the recommendation system is improved and the risk coefficient of the recommendation system is also reduced.

Acknowledgements

Supported by Tsinghua University Initiative Scientific Research Program (No. 20161080166)

References

[1] Qin Jiwei, Zheng Qinghua, et al., “A collaborative recommendation algorithm based on ratings and trust,” Joumal of Xi’an Jiaotong University, 2013, 47 (4), pp. 100-104.

[2] Liu Shengzong, Liao Zhifang, Wu Yanfeng, “A Collaborative Filtering Algorithm Combined with User Rating Credibility and Similarity,” Journal of Chinese Computer Systems, 2014, 35 (5), pp. 973-977.

[3] Miao Xinjie, The Research and Application of Collaborative Filtering Algorithm. Nanjing: Nanjing University of Information Science & Technology, 2014.

[4] R. Salakhutdinov, A. Mnih, and G. Hinton. Restricted boltzmann machines for collaborative filtering. In Proceedings of the 24th international conference on Machine learning, pp. 791–798. ACM, 2007.

[5] L. K. Saul, T. Jaakkola, and M. I. Jordan, Mean field theory for sigmoid belief networks. Arxiv preprint cs/9603102, 1996.

[6] Zhou Tao, Ren Jie, Medo M, et al., “Bipartite network projection and personal recommendation,” Physical Review E, 2007, 76 (4 Pt 2): 046115.

[7] Victor P, Verbiest N, Cornelis C, et al., “Enhancing the trust-based recommendation process with explicit distrust,” ACM Transactions on the Web (TWEB), 2013, 7 (2), pp. 61-80.

[8] Hinton G, Salakhutdinov R, “Reducing the dimensionality of data with neural network,” Science, 2006, 313 (504), Doi: 10, 1126/science, 1127647.

[9] Geoffrey E. Hinton, Simon Osindero, Yee-Whye The, “A Fast Learning Algorithm For Deep Belief Nets,” Neural Computation 18, 2006, pp. 1527-1554.

[10] Ruslan Salakhutdinov, Andriy Mnih, Geoffrey Hinton, “Restricted Boltzmann Machines for Collaborative Filtering,” Proceedings of the 24th International Conference on Machine Learning, Corvallis, OR, 2007.

[11] Yu Kai, Jia Lei, Chen Yuqiang, “Deep Learning: Promote the dream of artificial intelligence,” Programmer, 2013 (6), pp. 22-27.

[12] Wang Shengzhu, Li Yong-zhong, “Intrusion detection algorithm based on deep learning and semi-supervised learning,” Information Technology, 2017 (1), pp. 101-104, 108.

[13] Chen Hong, Wan Guangxue, “Intrusion detection method of deep belief network model based on optimization of data processing,” Journal of Computer Applications, 2017, 37 (6), pp. 1636-1643, 1656.