Identifying online user reputation in terms of user preference

Lu Dai [a], Qiang Guo [a], Xiao-Lu Liu [d], Jian-Guo Liu [b,*], Yi-Cheng Zhang [c]

[a] Research Center of Complex Systems Science, University of Shanghai for Science and Technology, Shanghai 200093, People's Republic of China
[b] Data Science and Cloud Service Research Centre, Shanghai University of Finance and Economics, Shanghai 200433, People's Republic of China
[c] Department of Physics, University of Fribourg, CH-1700 Fribourg, Switzerland
[d] School of Economics, Fudan University, Shanghai 200433, People's Republic of China

HIGHLIGHTS

- We present an improved group-based rating method for online ranking user reputation in terms of the user preference (PGR).
- By grouping users according to their mapped ratings, users are assigned with high reputation if they always fall into large rating groups.
- The AUC values of the PGR method can reach 0.9842 for malicious spammers, outperforming the traditional group-based method.

Identifying online user reputation is significant for online social systems. In this paper, taking into account the preference physics of online user collective behaviors, we present an improved group-based rating method for ranking online user reputation based on the user preference (PGR). All the ratings given by each specific user are mapped to the same rating criteria. By grouping users according to their mapped ratings, the online user reputation is calculated based on the corresponding group sizes. Results for MovieLens and Netflix data sets show that the AUC values of the PGR method can reach 0.9842 (0.9493) and 0.9995 (0.9987) for malicious (random) spammers, respectively, outperforming the results generated by the traditional group-based method, which indicates that the online preference plays an important role for measuring user reputation.

1. Introduction

Evaluating online user reputation in terms of the physics of their rating behaviors is of great significance for the online rating systems [1–5]. The ratings given to an object play an important role for other users' decisions. However, the ratings given by different users have their specific meaning since users have their specific interests and tastes [6–9].

Various reputation generation methods have been proposed. Laureti et al. [10] designed an iterative refinement (IR) method to measure online user reputation, where the user's reputation is inversely proportional to the difference between his ratings and the corresponding objects' estimated quality. The object quality and the reputation can be iteratively updated until they become stable. Zhou et al. [11] developed a correlation based ranking method (CR), where the user's reputation is determined by the Pearson correlation coefficient between his ratings and the objects' calculated quality. Liu et al. [12] presented an improved iterative algorithm for online ranking object quality and user reputation in terms of the user degree

---

* Corresponding author.
  E-mail address: liujg004@ustc.edu.cn (J.-G. Liu).
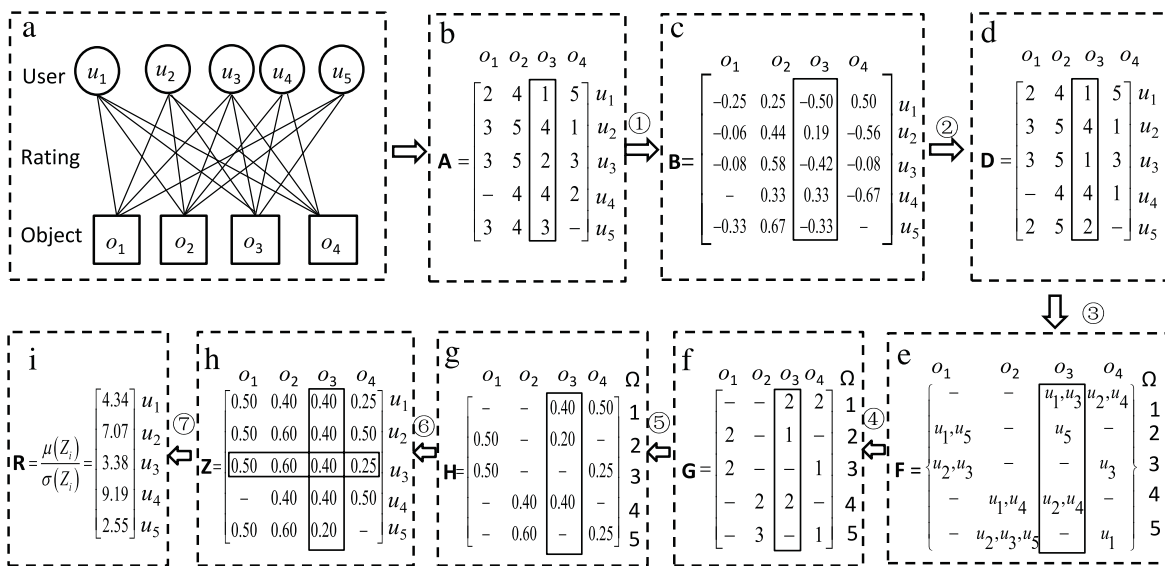
Fig. 1. A illustration of the PGR method. The arrow marks the step of the procedure. (a) The original bipartite network of the online rating system. (b) The corresponding rating matrix, **A**. The column and row correspond to objects and users, respectively. The symbol "-" stands for a non-rating. (c) After using a mapped method ($r_{i\alpha} - \mu_i)/(r_i^{max} - r_i^{min}$) to transform ratings, the mapped matrix **B** is established. (d) The new rating matrix **D**, transformed by matrix **B** referring to the class interval τ. Take o_3 as an example. $\tau = (0.50 + 0.50)/5 = 0.20$, $r'_{13} \in [-0.50, -0.30)$, $r^*_{13} = 1$. (e) The groups of users, F, after being grouped according to their processed ratings. Take o_3 as an example. As u_1 and u_3 rated 1 to o_3, they are put into group $F_{1,3}$. (f) The sizes of groups, **G**, $G_{1,3} = 2$ according to $F_{1,3} = \{u_1, u_3\}$. (g) The rating-rewarding matrix, **H**, established by normalizing **G** by column, e.g., $H_{1,3} = 2/(2 + 1 + 2) = 0.40$. (h) The rewarding matrix, **Z**, obtained by matrix **D** and **H**. The rewarding that user i obtain from his rating $r^*_{i\alpha}$ is defined as $Z_{i\alpha} = H_{s\alpha}$, where $r^*_{i\alpha} = r_s$, e.g. $r^*_{13} = 1$, $Z_{1,3} = H_{1,3} = 0.40$. (i) The reputation matrix **R**. Take u_3 as an example, $R_3 = \mu(Z_3)/\sigma(Z_3) = 3.38$.

(IRUA). The non-iterative online user reputation ranking methods are also discussed. Gao et al. [13] proposed a group-based ranking method (GR) by grouping users according to their ratings, where the user reputations could be determined by the corresponding group sizes, which is more accurate and robust than the CR method for the spamming attacks. Recently, Liu et al. [14] presented a ranking method based on the beta distribution (RBPD), where the user reputation is calculated as the probability that their ratings consistent with the main part of all user opinions.

Different users have different rating preference [14], some users prefer to give high ratings and others prefer to give low ratings. Liu et al. [9] found that besides the common tastes, more importantly, online users have their specific tastes. Hou et al. [15] empirically investigated the memory effect of online ratings and found that the user selecting behaviors could be regenerated by a Markovian model. Zhang et al. [16] found that large-degree users are stricter with their ratings so that they usually prefer to give lower ratings whatever the objects are, and vice versa. It should be noticed that the GR method calculated the online user reputation based on the idea that the rating value given by different users represents exactly same preference regardless the preference diversity. Inspired by the idea that the online user should be divided into groups according to their specific preference, in this Letter, we present an improved group-based rating method to measure online user reputation based on the user preference, namely PGR method. Firstly, all the ratings given by each specific user are mapped to the same rating criteria. Then, by grouping users according to their processed rating, we put users who gave the same ratings to one object into one group. Finally, the online user reputation could be calculated based on the corresponding group sizes. The experimental results for the MoiveLens and Netflix data sets show that the PGR method is more accurate and robust than the original group-based ranking method for the spamming attacks.

2. The PGR method

The online rating system can be described by a weighed bipartite network, where the users are denoted by set $U = \{u_1, u_2, \ldots, u_m\}$, objects are denoted by set $O = \{o_1, o_2, \ldots, o_n\}$, and the links between the user and object sets, are indicated by $E = \{e_1, e_2, \ldots, e_l\}$. Here, we use Latin and Greek letters, respectively, for user-related and object-related indices. The degrees of user i and object α are denoted as k_i and ρ_α. The bipartite network can be described as a rating matrix **A**, where the element $r_{i\alpha} \in \Omega = \{r_1, r_2, \ldots, r_z\}$ is the rating given by user i to object α. We use r_1 and r_z to represent minimum and maximum ratings, respectively, for online system. The reputation of user i is denoted as R_i.

Since different users have different rating preference, where some users tend to give high ratings and others tend to give low ratings. The quantity $r'_{i\alpha}$ is defined as the mapped rating for the original rating $r_{i\alpha}$, from which one can discover the opinion from user i to object α. The mapping process could be demonstrated as follows.

Step 1: We use a mapped method to transform ratings in the following way,

$$r'_{i\alpha} = \begin{cases} \dfrac{r_{i\alpha} - \mu_i}{r_i^{max} - r_i^{min}} & \text{if } r_i^{max} \neq r_i^{min} \\ 0 & \text{if } r_i^{max} = r_i^{min}, \end{cases} \tag{1}$$

where μ_i, r_i^{max} and r_i^{min} denote the average, maximum and minimum ratings user i given, respectively. We get a mapped rating matrix $\mathbf{B} = \{r'_{i\alpha}\}$. Specifically, for the users who always give the same ratings, their ratings are set to 0.

Step 2: We calculate a class of interval τ:

$$\tau = \frac{r'_{max} - r'_{min}}{l}, \tag{2}$$

where r'_{max} and r'_{min} denote the maximum and minimum mapped ratings given by all users, l is defined as the numbers of rating values for the online rating system. Then a new rating matrix $\mathbf{D} = \{r^*_{i\alpha}\}$ could be constructed by transforming the mapped ratings to online ratings, $[r'_{min}, r'_{min} + \tau), [r'_{min} + \tau, r'_{min} + 2\tau), \ldots, [r'_{min} + (l-1)\tau, r'_{max}]$ corresponding to $r_1, r_2, \ldots, r_z$.

Step 3: Users who gave the same rating to one object belong to the group $F_{s\alpha}$:

$$F_{s\alpha} = \{u_i | r^*_{i\alpha} = r_s\}, \tag{3}$$

Step 4: We calculate the number of users who gave the rating r_s to object α $G_{s\alpha} = |F_{s\alpha}|$.

Step 5: A rating-rewarding matrix $\mathbf{H}$ is constructed by normalizing matrix $\mathbf{G}$ by column:

$$H_{s\alpha} = \frac{G_{s\alpha}}{\rho_\alpha}, \tag{4}$$

where ρ_α is the degree of object α.

Step 6: Based on the rating-rewarding matrix $\mathbf{H}$ and the new rating matrix $\mathbf{D}$, we established a rewarding matrix $\mathbf{Z}$. The rewarding that user i obtain from his rating $r^*_{i\alpha}$ is defined as $Z_{i\alpha} = H_{s\alpha}$, where $r^*_{i\alpha} = r_s$.

Step 7: The reputation of users is correlative with their rewarding vectors. As a user whose average rewarding is small should have a lower reputation, because most of his ratings are deviated from the majority. In addition, if the rewarding varies largely, he also get a lower reputation for his unstable rating behaviors. In terms of the above process, the reputation R_i for user i is defined as

$$R_i = \frac{\mu(Z_i)}{\sigma(Z_i)}, \tag{5}$$

where σ and μ are standard deviation and mean value, respectively. Specifically, the mean value of Z_i is defined as

$$\mu(Z_i) = \sum_\alpha \frac{Z_{i\alpha}}{k_i}, \tag{6}$$

and the standard deviation of Z_i is defined as

$$\sigma(Z_i) = \sqrt{\frac{\sum_\alpha (Z_{i\alpha} - \mu(Z_i))^2}{k_i}}. \tag{7}$$

The calculation process of the PGR method is given in Fig. 1.

3. Data and metric

We investigate the performance of the PGR method for two empirical data sets: MovieLens and Netflix. The MovieLens data set is released by the GroupLens project at University of Minnesota (www.grouplens.org). The MovieLens ratings are given by the integer rating scale from 1 to 10 and each user has at least 20 ratings. Netflix is a data set provided by the DVD rental company Netflix for its Netflix Prize contest (www.netflixprize.com). The Netflix ratings are given by the integer ratings scaling from 1 to 5. We sampled and extracted a smaller data set from the original data set, respectively, by choosing users who have at least 20 rating and the movies are rated by at least one of these users. The basic statistics of data sets are summarized in Table 1.

3.1. Artificial spammers

There are two types of distorted ratings commonly existing in real online rating systems, namely, random ratings and malicious ratings. The random spammers who like to give casual ratings without reasons [7,17]. The malicious spammers always give maximum (minimum) allowable ratings to push up (down) certain target objects. These dishonest ratings influence the accuracy of ranking methods [17,18], a good ranking method should be robust against any kind of

Table 1
Basic statistical properties of the MovieLens and Netflix data sets. m is the number of users, n is the number of objects. The quantities $\langle k_u \rangle$ and $\langle \rho_o \rangle$ denote the average degrees of users and objects. The Sparsity is the proportion of the number of links in the maximum possible number of links.

Data set	m	n	$\langle k_u \rangle$	$\langle \rho_o \rangle$	Sparsity
MovieLens	668	10 325	158	10	0.015
Netflix	4323	13 250	205	67	0.012

spammers [19–21]. In fact, we are unable to pick up spammers from all users in advance. To test the performance of different ranking methods, we put two types of artificial spammers(malicious or random) into the real data sets.

In the calculation process, we randomly select d users as spammers and replace their original ratings with distorted ratings: (i) integer r_1 or r_z with the same probability (i.e., 0.5) for malicious spammers, and (ii) random integers in $r_1, r_2, r_3, \ldots, r_z$ for random spammers. The activities of spammers is denoted as $p = k/n$, where k is the degree of each spammer. The ratio of spammers is denoted as $q = d/m$.

3.2. Evaluation metric

The AUC metric [22] is introduced to measure the accuracy of ranking methods. To calculate the AUC value, one should randomly pick a spammer and a normal user to compare their reputations at each time. After s times of independent comparisons, we record s_1 as the number of times in which the spammer has a lower reputation, and s_2 as the number of times in which the spammer and normal user have the same reputation. In short, the AUC value can be described as the probability that the reputation of a randomly chosen spammer is lower than that of a randomly chosen normal user. The final AUC value is calculated as

$$AUC = \frac{s_1 + 0.5s_2}{s}. \tag{8}$$

When AUC = 1, all the spammers are ranked lower than the normal users. While AUC = 0.5 indicates all the users and spammers are ranked randomly.

When we evaluate the online user reputation, there is an intuition that a user with lower reputation should have a higher rating error and vice versa. In other words, if the calculated reputation R_i is negatively correlated with the rating error δ_i, the method can be considered well-performed. In this Letter, the rating error of a user is defined as the degree of deviation after comparing the estimated objects quality $\overline{Q}_\alpha$ and the rating $r_{i\alpha}$. Here, we take the average rating as objects quality $\overline{Q}_\alpha$. Mathematically, the rating error of user i is defined as

$$\delta_i = \frac{\sum_\alpha |r_{i\alpha} - \overline{Q}_\alpha|}{k_i}, \tag{9}$$

where $\overline{Q}_\alpha = \sum_{i \in U_\alpha} r_{i\alpha} / \rho_\alpha$ is the average rating of object α, and U_α is the user set who gave ratings to object α. The Pearson correlation coefficient C between R_i and δ_i is defined as

$$C = \frac{1}{m} \sum (\frac{R_i - \overline{R}}{\sigma_R})(\frac{\delta_i - \overline{\delta}}{\sigma_\delta}), \tag{10}$$

where m is the number of users, σ_R and σ_δ represent the standard deviations of the reputations and rating errors of all users, respectively. Meanwhile, the quantities $\overline{R}$ and $\overline{\delta}$ are their mean values. The Pearson correlation coefficient C can measure the reliability of a ranking method. The higher the correlation is, the more reliable the method is.

4. Results

To compare the performance of different ranking methods, we calculate the Pearson correlation coefficient C between δ_i and R_i. For the MovieLens and Netflix data sets, the correlation $C = -0.559\,(-0.354)$ and $-0.845\,(-0.684)$ for the PGR (GR) method. We can find that both two methods assign a high reputation to users of low rating errors and a low reputation to users of high rating errors. The larger negative correlation indicates that the PGR method is better for evaluating the online user reputation.

4.1. Reputation evaluation

We investigate the robustness of the PGR and GR methods for different ratio of objects rated by spammers p and ratio of spammers q. When $p = 0.01$ and $q = 0.02$, the result shows that the AUC values of the PGR method can reach 0.9842 (0.9493) and 0.9995 (0.9987) for malicious (random) spammers for the MovieLens and Netflix data sets, respectively, which outperforms the GR method. Fig. 2 shows the AUC values of the PGR and GR methods for the MovieLens data set, from which
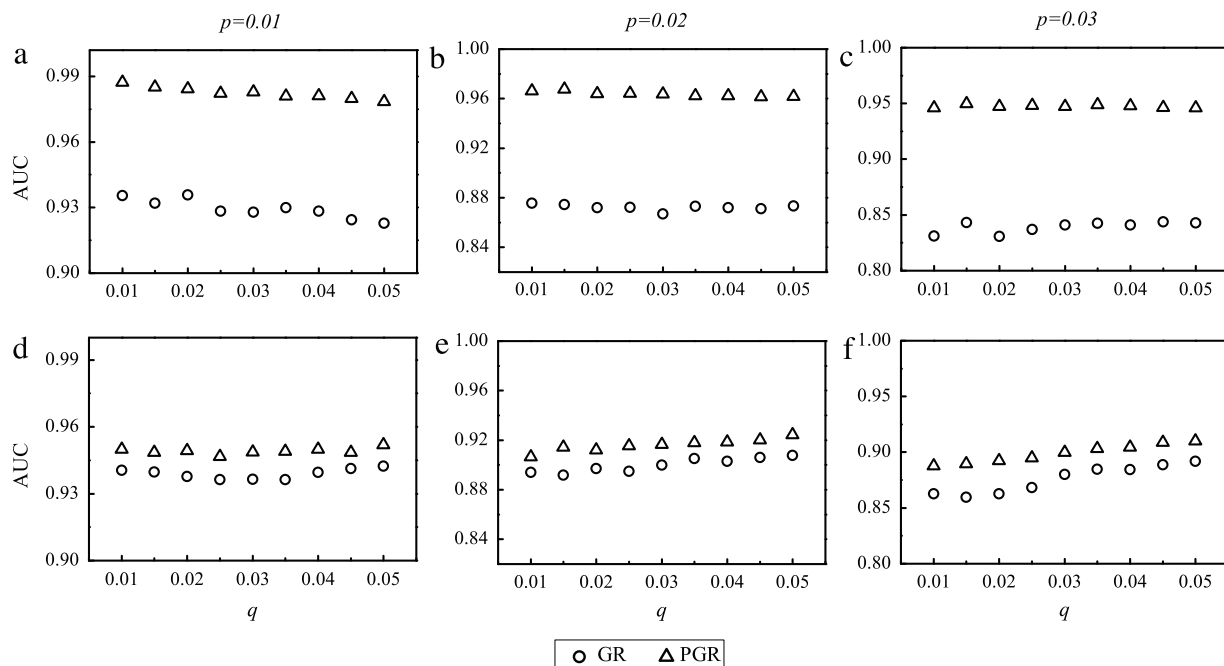
Fig. 2. The AUC values of the PGR and GR methods for the MovieLens data set, where the parameters q and p are ratio of spammers and ratio of objects rated by spammers, respectively. The subplots (a)–(c) show the AUC values for the malicious spammers, the subplots (d)–(f) show the AUC values for the random spammers. One can find that the AUC values of the PGR method are larger than those of the GR method for different parameters p and q. The results are averaged over 100 independent realizations.
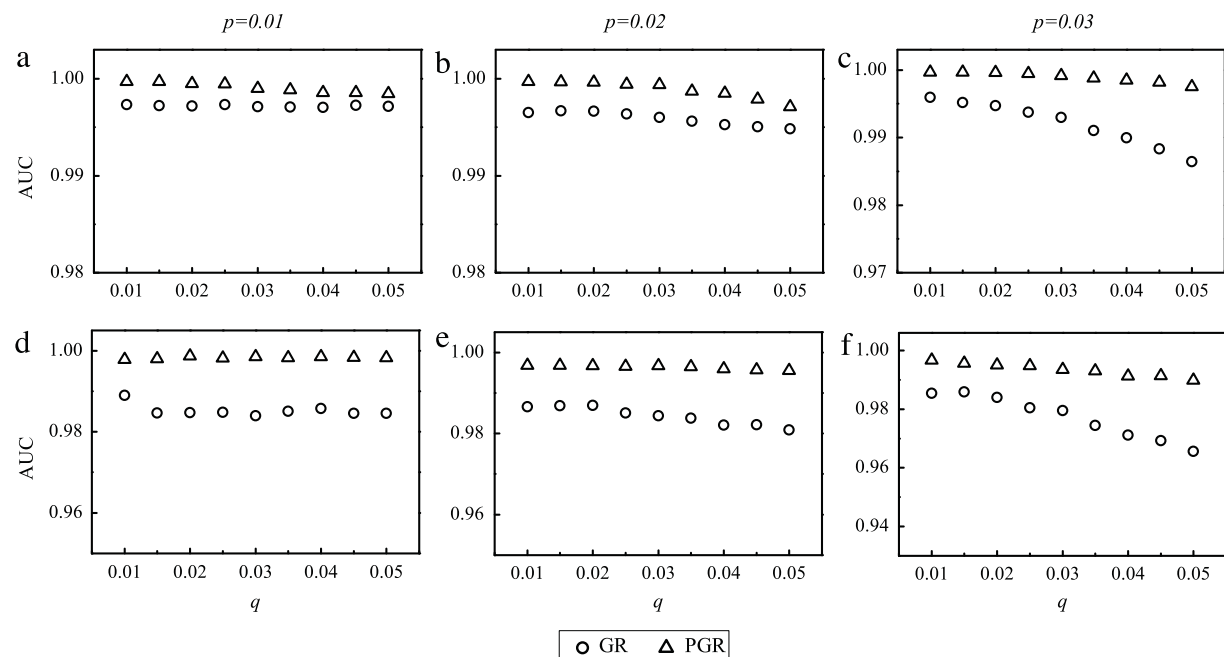
Fig. 3. The AUC values of the PGR and GR methods for the Netflix data set, where the parameters q and p are ratio of spammers and ratio of objects rated by spammers, respectively. The subplots (a)–(c) show the AUC values for the malicious spammers, the subplots (d)–(f) show the AUC values for the random spammers. One can find that the AUC values of the PGR method are larger than those of the GR method for different parameters p and q. The results are averaged over 100 independent realizations.

one can find that for both malicious and random spamming attacks, the AUC values of the PGR method are larger than the ones obtained by the GR method for different parameters p and q. The results for the Netflix data set are shown in Fig. 3,

5
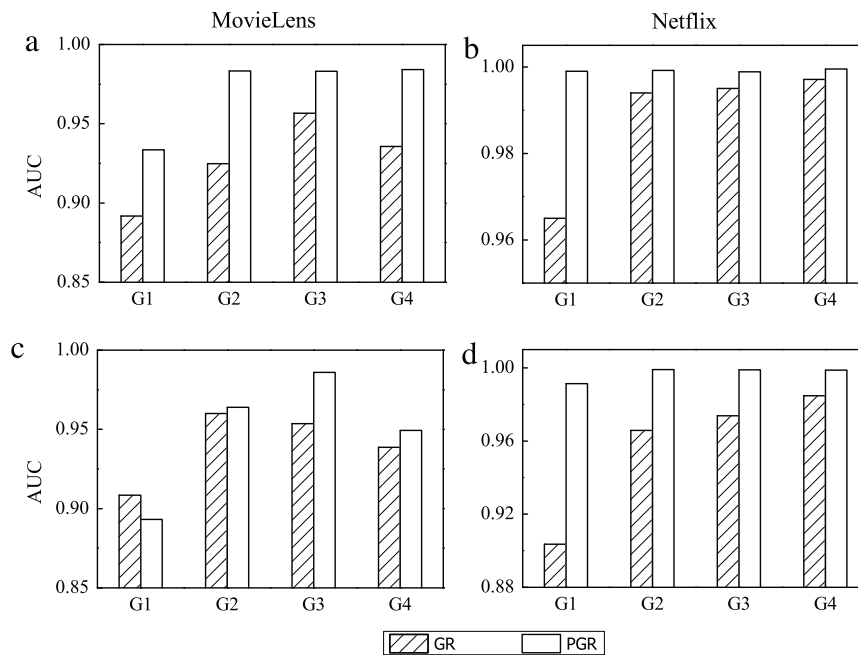
Fig. 4. The AUC values of different user groups for the MovieLens and Netflix data sets. The subplots (a) and (b) show for malicious spammers, the subplots (c) and (d) show for random spammers. According to degree intervals [0, 100), [100, 300) and [300, k^{max}], all users (G4) are divided into three groups, namely, G1, G2 and G3. For the MovieLens data set, one can find that the AUC values of the PGR method are larger than the ones obtained by the GR method except for small-degree users for random spammers. For the Netflix data set, the AUC values of the PGR method are larger than GR method in each group for both malicious and random spammers. The PGR method outperforms than the GR method in ranking all users. The parameter $p = 0.01$, $q = 0.02$. The results are averaged over 100 independent realizations.

Table 2
The AUC values of different parameters l ($l = 2, 4, 5, 8, 10$) for the MovieLens and Netflix data sets. One can find that the AUC value reach the largest value when $l = 5$ for both malicious and random spamming attacks. The AUC value of the PGR method for the empirical data sets with $p = 0.01$, $q = 0.02$. The results are averaged over 100 independent realizations.

Data set	Malicious spammers					Random spammers				
	2	4	5	8	10	2	4	5	8	10
MovieLens	0.9108	0.9792	**0.9921**	0.9881	0.9842	0.8835	0.9482	**0.9752**	0.9567	0.9493
Netflix	0.9376	0.9993	**0.9995**	0.9927	0.9965	0.9261	0.9982	**0.9987**	0.9983	0.9969

from which one can find that for malicious and random spammers the AUC values of the PGR method are also larger than those of the GR method.

Users with different degrees have different characteristics in online rating systems [9,23]. We explore the performance of the PGR and GR methods for users with different kinds of degrees. Since only a small number of users have large degrees, to trade off the number of users in each group, all users (G4) are divided into G1,G2 and G3 groups according to degree intervals [0, 100), [100, 300) and [300, k^{max}], where k^{max} is the maximum value of the user degree k_i. The AUC values are calculated by using the PGR and GR methods for each group. Fig. 4 shows the AUC values of the PGR and GR methods in each of groups for the MovieLens and Netflix data sets. For the MovieLens data set, we find that the AUC values of the PGR method are larger than those of the GR method except for small-degree users for the random spammers. For the Netflix data set, the results show that, in each group, the AUC values of the PGR method are larger than the ones obtained by the GR method for both malicious and random spammers.

4.2. The different numbers of rating values

For the MovieLens and Netflix data sets, the users could rate objects in 10 and 5 discrete values. Different numbers of rating values may affect the performance of the PGR method. We investigate the AUC values of the PGR method with different parameter l. Table 2 shows the results, from which we can find that one has the highest AUC values when $l = 5$, which suggests that the PGR method has the best performance for 5 rating values.

5. Conclusion and discussions

In this Letter, we propose an improved group-based rating method (PGR) for identifying online user reputation based on the specific tastes for different users. Firstly, we map all ratings to the same rating criteria. Then, by grouping users according to their processed ratings, a rating-rewarding matrix is established based on the corresponding group sizes. Finally, the online user reputation is defined as the inverse of dispersion of frequency distribution of his rewarding vector. The experimental results for the empirical networks show that the AUC values of the PGR method can reach 0.9842 (0.9493) and 0.9995 (0.9987) for the malicious (random) spammers for the MovieLens and Netflix data sets when $p = 0.01$, $q = 0.02$, where the parameters q and p are ratio of spammers and ratio of objects rated by spammers. Meanwhile, extensive experiments show that the PGR method outperforms the GR method in resisting spamming for different parameters q and p. In addition, we explore the effects of different numbers of rating values for the PGR method. When the number of rating values $l = 5$, the AUC values reach the largest values 0.9921 (0.9752) and 0.9995 (0.9987) for malicious (random) spammers for the MovieLens and Netflix data sets, respectively, which suggests that 5 rating values outperforms other groups in reputation identification for the PGR method.

Although the PGR method could outperform the traditional GR method, there are still some points which should be addressed in the future work. Different objects have different popularity mechanisms [24]. Since the performance of the reputation identification also depends on the object quality measurement, the influence of the popularity dynamics for the online user reputation measurement should be investigated. In this Letter, the rating map function introduced in Eq. (1) helps to increase the performance. How to find the concrete way to map the user preference more objectively is another promising way. More importantly, how to design an adaptive reputation system to objectively reflect the real reputation of users in terms of their interest evolution [14,25] and research the influence of community structures [26] would be investigated in the future.

References

[1] T. Zhou, Z. Kuscsik, J.G. Liu, M. Medo, J.R. Wakeling, Y.C. Zhang, Solving the apparent diversityCaccuracy dilemma of recommender systems, Proc. Natl. Acad. Sci. USA 107 (10) (2010) 4511–4515.
[2] L. Muchnik, S. Aral, S.J. Taylor, Social influence bias: a randomized experiment, Science 341 (6146) (2013) 647–651.
[3] M. Medo, J. Wakeling, The effect of discrete vs. continuous-valued ratings on reputation and ranking systems, Europhys. Lett. 91 (2010) 48004.
[4] Z. Yang, Z.K. Zhang, T. Zhou, Anchoring bias in online voting, Europhys. Lett. 100 (2012) 68002.
[5] S. Cuomo, P.De. Michele, F. Piccialli, A. Galletti, J.E. Jung, IoT-based collaborative reputation system for associating visitors and artworks in a cultural scenario, Expert Syst. Appl. 79 (2017) 101–111.
[6] Z. Noorian, J. Zhang, Y. Liu, S. Marsh, M. Fleming, Trust-oriented buyer strategies for seller reporting and selection in competitive electronic marketplaces, Auton. Agents Multi-Agent 28 (2014) 896–933.
[7] Q.M. Zhang, A. Zeng, M.S. Shang, Extracting the information backbone in online system, PLoS One 8 (2013) e62624.
[8] M. Allahbakhsh, A. Ignjatovic, An iterative method for calculating robust rating scores, IEEE Trans. Parallel Distrib. 26 (2015) 340–350.
[9] J.G. Liu, T. Zhou, Q. Guo, Information filtering via biased heat conduction, Phys. Rev. E 84 (2011) 037101.
[10] P. Laureti, L. Moret, Y.C. Zhang, Y.K. Yu, Information filtering via iterative refinement, Europhys. Lett. 75 (6) (2006) 1006.
[11] Y.B. Zhou, T. Lei, T. Zhou, A robust ranking algorithm to spamming, Europhys. Lett. 94 (2011) 48002.
[12] X.L. Liu, Q. Guo, L. Hou, C. Cheng, J.G. Liu, Ranking online quality and reputation via the user activity, Physica A 436 (2015) 629–636.
[13] J. Gao, Y.W. Dong, M.S. Shang, S. Cai, T. Zhou, Group-based ranking method for online rating systems with spamming attacks, Europhys. Lett. 110 (2015) 28003.
[14] X.L. Liu, J.G. Liu, K. Yang, Q. Guo, J.T. Han, Identifying online user reputation of userCobject bipartite networks, Physica A 467 (2017) 508–516.
[15] L. Hou, X. Pan, Q. Guo, J.G. Liu, Memory effect of the online user preference, Sci. Rep. 4 (2014).
[16] Y.L. Zhang, Q. Guo, J. Ni, J.G. Liu, Memory effect of the online rating for movies, Physica A 417 (2015) 261–266.
[17] A. Zeng, G. Cimini, Removing spurious interactions in complex networks, Phys. Rev. E 85 (2012) 036101.
[18] D.D. Zhao, A. Zeng, M.S. Shang, J. Gao, Long-term effects of recommendation on the evolution of online systems, Chin. Phys. Lett. 30 (11) (2013) 118901.
[19] B. Li, R.H. Li, I. King, M.R. Lyu, J.X. Yu, A topic-biased user reputation model in rating systems, Knowl. Inf. Syst. 44 (2015) 581–607.
[20] A. Galletti, G. Giunta, G. Schmid, A mathematical model of collaborative reputation systems, Int. J. Comput. Math. 89 (2012) 2315–2332.
[21] F. Fouss, Y. Achbany, M. Saeren, A probabilistic reputation model based on transaction ratings, Inform. Sci. 180 (2010) 2095–2123.
[22] J.A. Hanley, B.J. McNeil, The meaning and use of the area under a receiver operating characteristic (ROC) curve, Radiology 143 (1) (1982) 29–36.
[23] J. Ni, Y.L. Zhang, Z.L. Hu, W.J. Song, L. Hou, Q. Guo, J.G. Liu, Ceiling effect of online user interests for the movies, Physica A 402 (2014) 134–140.
[24] J.P. Gleeson, D. Cellai, J.P. Onnela, M.A. Porter, F. Reed-Tsochas, A simple generative model of collective online behavior, Proc. Natl. Acad. Sci. 111 (2014) 10411–10415.
[25] T. Jia, D. Wang, B.K. Szymanski, Quantifying patterns of research-interest evolution, Nat. Hum. Behav. 1 (2017) 0078.
[26] K. Yang, Q. Guo, S.N. Li, J.T. Han, J.G. Liu, Evolution properties of the community members for dynamic networks, Phys. Lett. A 381 (2017) 970–975.