ISSN:0975-9646

Trust Aware Recommender Systems: A Survey on Implicit Trust Generation Techniques

Swati Gupta, Sushama Nagpal
Division of Computer Engineering, Netaji Subhas Institute of Technology, New Delhi-110078

***Abstract*—Development of Web 2.0 enabled users to share information online, which results into an exponential growth of world wide web data. This leads to the so-called information overload problem. Recommender Systems (RS) are intelligent systems, helping on-line users to overcome information overload by providing customized recommendations on various items. In real world, people are willing to take advice and recommendation from their trustworthy friends only. Trust plays a key role in the decision-making process of a person. Incorporation of trust information in RS, results in a new class of recommender systems called trust aware recommender systems (TARS). This paper presents a survey on various implicit trust generation techniques in context of TARS. We have analyzed eight different implicit trust metrics, with respect to various properties of trust proposed by researchers in regard to TARS.**

Keywords*—implicit trust; trust aware recommender system; trust metrics.

I. Introduction

During the last two decades, rapid evolution of information technology has brought tremendous change in all sectors of modern society. Information sharing in the Web is getting enormous. Web 2.0 applications allow millions of users to publish and edit content as well as to share data in an uncontrolled way. A single e-commerce web site can offer up to millions of items in different categories and for different types of users. This exponential growth of information has led to the information overload problem, i.e. the inability to cope with and manage all the available information in an efficient way [1].

Recommender systems (RS) provide a solution to information overload problem by customizing recommendations as per user 's preference. RS are intelligent applications that are able to identify and suggest the products, information or services that best fit the user's needs. RS not only save user's time but are also important from business point of view. RS play important role in influencing the profit percent of online retailers. RS also play an important role in critical decision making of a person. Stachowiak et.al. [29] designed an election recommendation system based on IF-set theory, which is supposed to help voters in deciding right candidate to vote for, as per their preferences.

In this paper, our focus is on Implicit Trust Aware Recommendation Systems(ITARS). This paper presents a survey on various implicit trust generation techniques, proposed by researchers in regard to trust aware recommender systems. The organization of paper is as follows: Section-II demonstrates traditional recommendation approaches along with their limitations. Section-III presents a review of trust definition and properties. Architecture of trust aware recommender system is also presented along with the limitations of explicit trust. Section-IV presents eight most popular implicit trust generation metrics, to extract trust from user-item ratings. We have classified implicit trust metrics in terms of trust properties in context of TARS. Section-V represents discussion on paper. In section-VI final conclusions are provided.

II. Recommendation Approaches

Recommender System is an active and fast growing field of research. The two major methods for generating recommendations are the content-based and collaborative filtering.

Content Based (CB) Filtering technique analyze item 's attributes to identify items, which are of a particular interest, to the target user [7]. CB systems do not show serendipity [8]. The main limitation of CB recommender system is that they require description of content of items and hence are not highly scalable.

Collaborative Filtering (CF) simulates a simple and effective social strategy called *word-of-mouth* [3], [4]. The main concept behind CF is that users with similar ratings in past are more likely to have similar ratings in future [5]. CF is classified into the memory based and model based techniques [6]. Memory based CF falls in the class of Machine Learning techniques called lazy learners (or k-nearest neighborhood). Pure memory based methods require no computation at model building time, as they provide rating prediction based on the ratings of similar users, which are computed at run time. Conversely, model based techniques use training data set to build a predictive model, which is later used to generate recommendations.

CF is the most successful and widely applied recommendation generation technique. CF requires no prior knowledge of the application domain and is highly scalable. Tapestry [2] is a popular CF based recommender system.

Despite the continuous research and a variety of approaches, recommender systems still face limitations. These limitations are summarized in following subsection.

A. Limitations of Typical Recommender Systems

Recommender systems, in particular, collaborative filtering based recommender systems, face three major challenges: cold start, data sparsity, and attack [4], [9], [19]:

1) The cold start problem: This refers to the inability in generating good quality recommendations for a new user or a user with low activity.

2) Sparsity: It refers to the sparsity of user-item rating matrix, because of unwillingness of users towards providing ratings. Sparsity results in difficulty of finding similar users which will further need to participate in generation of recommendations for active user.

3) Malicious Attacks: CF recommender systems are prone to malicious attacks. Copy profile is an example of such attack.

4) Lack of transparency: Users are unaware of the recommendation generation process and they have no control over it. This decreases trust of users, on the recommendations generated by the system.

A solution to overcome these limitations of traditional recommender systems, is to incorporate trust relationships in recommender systems, resulting trust-based or trust-aware recommender systems [9].

III. About Trust

Trust plays an important role across many disciplines, and forms an important feature of our everyday lives. In addition, trust is a property associated with people in the real world as well as users in social media [10], [13]. In recommender systems, it is defined based on the other users' ability to provide valuable recommendations [11].

Marsh [12] introduced trust as a computational concept. Marsh also introduced the distrust as the negative trust.

The trust value can be either binary or real numbers (i.e., in the range of [0; 1]). Binary trust is the simplest way of expressing trust. Either two users trust each other or not. A more complicated method is continuous trust model, which assigns real values to the trust relations. In both binary trust and continuous models, 0 and 1 mean no trust and full trust, respectively. Some researchers also incorporated distrust (negative trust) to improve recommender system 's performance. Distrust lies in the range [-1; 0).

A. Computational Properties of Trust

In this section, we introduce core properties of trust with respect to TARS. These properties are extracted from trust definitions and provide the basis for the creation of algorithms, that utilize trust information in recommendation generation.

Properties of trust are as follows:

1) Asymmetry: Trust is a subjective and personal relation between users; therefore, it creates a directed relation in social networks. In other words, if $t_{u,v}$ represents the value of trust u have on v, it might not be equal to the value of trust v have on u. Hence, trust is directed and asymmetric.

2) Transitivity: Transitivity is a key property of trust. It allows trust to be propagated in the trust network. Based on the transitivity effect, if u trusts v and v trusts w, it can be inferred that u might also trust w to some extent.

3) Dynamicity: Trust is a dynamic quantity. It changes continuously with time. Positive facts increase trust while negative facts decrease trust.

4) Propagation: Propagation is a property of trust that benefits the process of predicting the trust score through known trust paths. Direct trust relations in a user 's trust network build a path through which new indirect connections can be established with other users. In past researchers have incorporated various methodologies for trust propagation. Genetic and optimization algorithm have been manifested for addressing the trust propagation. Bedi et.al. [27] incorporated ant colony optimization for trust propagation. Stachowiak [30] innovated fuzzy measure for trust propagation in social network.

5) Network Perspective: Global vs Local trust: Trust can be inferred through global or local trust measures. Local trust is the subjective measure of a user for the trustworthiness of another user. In other words it is the degree of a trust relationship between two users. Global trust, on the other hand, is the consensus of the whole community about the trustworthiness of a user. Global trust is the reputation that a user has in the network. In trust aware recommender system literature local trust metric is generally preferred although there are systems that adopt both local and global trust.

6) Trust establishment: Explicit vs Implicit trust: Trust establishment can be based on explicit or implicit trust networks. Explicit networks are built with explicit trust statements, which are directly provided by a user for another user. Whereas implicit trust scores are inferred from user 's behavior. Implicit trust relationships are computed through user similarity and other trust metrics. Explicit and implicit trust can be either bivalent or expressed in a gradual scale. Several studies [15], [20], [16] use explicit trust however, several other [19], [22], [18], [24], [21], [23] infer trust relationships to build the implicit trust.

7) Context dependency: Trust is context dependent. This means that trusting someone on one topic does not guarantee trusting him in other topics as well. For example, one who is trustworthy in technology might not be trustworthy in astronomy.

B. Trust Aware Recommender System

It is common in real life to take advices on topics we are not expert in from trustworthy friends. Trust-Aware recommender system (TARS) is basically an evolution of traditional collaborative filtering based recommender systems. TARS consider trust relationship among users in order to generate recommendations [20]. Since trust can be propagated in network, hence TARS can easily overcome data sparsity and cold start problems from which traditional CF suffer [16], [9]. Trust can be either explicit or implicit.

1) Explicit trust: Explicit trust is the trust value explicitly provided by the users. For example, users in FilmTrust [15] rate other users by providing trust scores. Many explicit trust-based recommender systems have been proposed in literature [16], [15], [20]. Figure 1 shows architecture of Explicit Trust Aware Recommender System.

2) Implicit trust: It refers to the trust information implicitly inferred from user behavior in the system e.g. user-item ratings. Many implicit trust-based recommender systems have been proposed in literature [19], [22], [18], [24], [21], [23]. Figure 2 shows architecture of Implicit Trust Aware Recommender System.

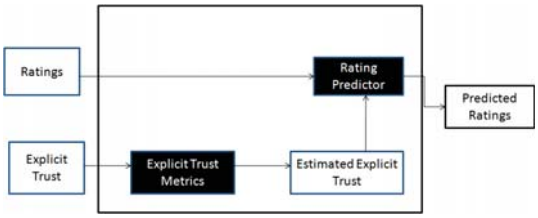

Fig. 1. Explicit Trust Aware Recommender System Architecture.

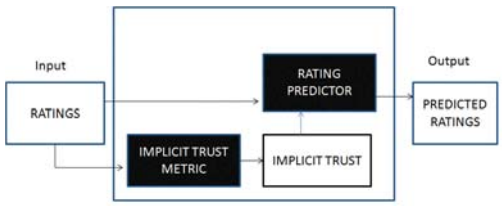

Fig. 2. Implicit Trust Aware Recommender System Architecture.

C. Limitations of Explicit Trust

There exist several limitations of explicit trust [11], [16], [26], [18]. This section highlights the major limitations of explicit trust:

1) Extra User Effort: Explicit trust puts extra burden on user for providing trust information apart from rating information [26].

2) Unavailability: Some popular datasets available for research purpose lack explicit trust information. E.g. Datasets like Jester do not contain trust information.

3) Binary Nature of Trust in Datasets: Most of the publicly available explicit trust datasets contain trust score in binary form. For example FilmTrust and Epinions contain binary values of trust. This indifferent nature of trust, inhibits the recommender system from achieving better performance.

4) Noisy: Sometimes explicit trust could be noisy. Users may trust each other due to various offline relations. But this does not confirm that they have same taste and their preferences are also same i.e. trust in a person is different than trust in a person's recommendation.

5) Sparsity of Explicit Trust Information: The amount of explicit trust information is relatively less than the number of ratings. Though trust propagation can resolve this issue to some extent, it is risky to raise new noise [16].

Due to the limitations of explicit trust as discussed above, lots of research has been carried out in the area of generating trust implicitly from user behavior [19], [22], [18], [24], [21], [23]. In our recent work [28], we have provided an empirical analysis of various implicit trust metrics on two different real world datasets.

Following section discuss popular implicit trust generation techniques, proposed by researchers.

IV. Implicit Trust Metrics

Implicit trust metrics are based on the instinct that the users with similar ratings tend to be trustworthy [14]. Various trust metrics are proposed in literature to calculate implicit trust from user - item ratings. In this survey, we have elaborated eight different metrics for trust generation.

A. Literature of Eight Popular Implicit Trust Metrics

Before discussing the literature of implicit trust metrics, some of the most common notations are presented as follows:

U: set of all users in the system.

I: set of all items in the system.

R: set of all ratings in the system.

Symbols u, v represents users and u, v ε U.

Symbols i, j represents items and i, j ε I.

$r_{u,i}$: u's rating score for item i.

I_u : set of items rated by user u.

$I_{u,v}$: set of items commonly rated by users u and v.

$|I_{u,v}|$: number of items commonly rated by users u and v.

$t_{u,v}$: trust value of user u on user v.

$s_{u,v}$: similarity value of user u with user v.

θ_s : threshold for user similarity.

θ_I : threshold for co-rated items.

$\bar{r}_u$: mean rating of user u.

Eight popular implicit trust metrics (represented as M1-M8), proposed in literature are elaborated as follows.

1) M1: Lathia et al. [19] stress on importance of rating items, although opinions may be different. This metric has power of computing trust value between users who have rated even a single item in common. Hence, M1 has an extra advantage over similarity based matrices which generally fails to calculate trust when number of commonly rated items is less than a given threshold. Trust is defined as follows:

$$t_{u,v} = \frac{1}{|I_{u,v}|} \sum_{i \varepsilon I_{u,v}} (1 - \frac{|r_{u,i} - r_{v,i}|}{r_{max}}) \quad (1)$$

Here, r_{max} is the maximum allowed rating by a recommender system and other terms have their usual meaning as stated in beginning of this section. This metric to infer trust is symmetric, i.e. $t_{u,v} = t_{v,u}$. It is neither dynamic nor context sensitive [11]. Trust propagation is not considered in this metric. Experimental Results [19] have shown that using M1 trust metric prediction rating coverage has improved significantly. The reason behind this is that metric is able to compute trust even when user - item rating matrix is sparse. M1 has resolved data sparsity problem effectively, however cold start and vulnerability to attacks still need to be handled efficiently. Also M1 has neglected the concept of distrust completely, since negative trust cannot be generated via this metric.

2) M2: Papagelis et al. [22] derive trust via user similarity computed as Pearson correlation coefficient (PCC). M2 basically treats similarity values generated by PCC as trust and propagates these trust values over the network to generate inferred trust values, in order to eliminate data sparsity.

$$t_{u,v} = \frac{\sum_i (r_{u,i} - \bar{r}_u)(r_{v,i} - \bar{r}_v)}{\sqrt{\sum_i (r_{u,i} - \bar{r}_u)^2} \sqrt{\sum_i (r_{v,i} - \bar{r}_v)^2}} \quad (2)$$

Papagelis et al. [22] considers propagation of implicit trust generated. Trust values can be propagated only if they are positive in nature. Negative trust (distrust) is not propagated in network.

If direct trust values exist between users s and n i.e. $t_{s,n}$ and also direct trust exist between users n and t i.e. $t_{n,t}$. But there is no direct trust value between user s and t, and then trust can be propagated, to generate trust value between user s and t using following equation:

$$t_{s,t} = \frac{|I_{s,n}|}{|I_{s,n}| + |I_{n,t}|} t_{s,n} + \frac{|I_{n,t}|}{|I_{s,n}| + |I_{n,t}|} t_{n,t} \quad (3)$$

Papagelis et al. [22] introduced terms confidence and uncertainty, which are asymmetric in nature and used them for path composition and path selection, in case of multiple path existence.

3) M3: Yuan et al. [26] generates binary trust by setting a threshold value for similarity.

$$t_{u,v} = \begin{cases} 1, & \text{if } s_{u,v} > \theta_s, |I_{u,v}| > \theta_I \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

Similarity values are calculated using PCC in equation 2. In addition, Sotos et al. [25] results that PCC is transitive, only when it crosses a threashold, i.e. $s_{u,v}$ >0.707. Therefore θ_s is set as 0.707. Further, Guo et al. [17] revealed that there must be some threshold on commonly rated items to ensure the reliability of trust. The implicit trust generated is binary in nature. Yuan et al. [26] verified that trust network generated above fulfill the property of small worldness and this property is independent of the dynamics of implicit trust networks. Trust can be propagated in binary network using equation 5:

$$t_{s,t} = \frac{\lceil \log n / \log k \rceil - d_{u,v} + 1}{\lceil \log n / \log k \rceil} \quad (5)$$

Here, n is the size and k is the average degree of the implicit trust network. And $d_{u,v}$ is the trust propagation distance from u to v.

4) M4: Hwang and Chen [18] used Resnick's prediction formula for generating predicted rating.

$$p_{u,i} = \bar{r}_u + (r_{v,i} - \bar{r}_v) \quad (6)$$

The trust value is derived as follows:

$$t_{u,v} = \frac{1}{|I_{u,v}|} \sum_{i \varepsilon I_{u,v}} (1 - \frac{|p_{u,i} - r_{u,i}|}{r_{max}}) \quad (7)$$

Guibing et al. [11] report that trust computed is symmetric in nature, also dynamicity and context dependency are not taken into account. Hwang and Chen [18] also considered trust propagation in his study. Trust propagation is done to resolve the sparsity problem and to increase the rating coverage. Trust propagation is done using equation 3. In case multiple paths, average of all inferred trust scores is taken. Hwang and Chen [18] also have proposed a strategy for global trust computation, by averaging the local trust scores of users, who are directly connected to user for whom we need to calculate global trust score or reputation.

5) M5: Shambour and Lu [24] also used Resnick 's prediction formula for trust computation. Computed trust is based on mean squared distance (MSD):

$$t_{u,v} = \frac{|I_{u,v}|}{|I_u \cup I_v|} (1 - \frac{1}{|I_{u,v}|} \sum_{i \varepsilon I_{u,v}} (\frac{|p_{u,i} - r_{u,i}|}{r_{max}})^2) \quad (8)$$

The users whose trust score crosses threshold λ , i.e., $t_{u,v}$>λ are trusted neighbors and take part in trust propagation. Guibing et al. [11] report that trust computed is symmetric in nature, moreover dynamicity and context dependency are not taken into account while computing trust.

Shambour and Lu [24] proposed direct trust propagation to generate inferred trust. For rating prediction Shambour combined both similarity and trust. Shambour and Lu [24] also incorporated item based collaborative filtering (CF) along with, semantic information of items. A fusion of trust based CF and semantic item based CF is done for final rating prediction. Although, this approach solved the cold start and sparsity significantly, but computational cost is huge.

6) M6: Donovan and Smyth [21] defined two levels of trust i.e. profile level trust and item level trust. Rating is considered as correct if the prediction error is smaller than a given threshold ϵ

$$correct(r_{u,i}, r_{v,i}) \leftrightarrow |p_{u,i} - r_{u,i}| \leq \epsilon \quad (9)$$

Where, $p_{u,i}$ is given by Equation 6.

The profile-level trust is defined as:

$$t_{u,v} = \frac{|CorrectSet(v)|}{|RecSet(v)|} \quad (10)$$

Where CorrectSet(v) is correct ratings set provided by user v, and RecSet(v) is recommendation set in which user v has involved. This metric is symmetric [11]. Trust propagation is not taken into consideration.

7) M7: Pitsilis and Marshall [23] defined uncertainty as:

$$u_v = \frac{1}{|I_{u,v}|} \sum_{i \varepsilon I_{u,v}} (\frac{|p_{u,i} - r_{u,i}|}{r_{max}}) \quad (11)$$

Where u_v is the uncertainty of user u towards user v, and $p_{u,i}$ is derived from Equation 6. Pitsilis et. al. defined belief and disbelief as:

$$b_v = \frac{1}{2}(1 - u_v)(1 + s_{u,v}) \tag{12}$$

$$d_v = \frac{1}{2}(1 - u_v)(1 - s_{u,v}) \tag{13}$$

Where similarity is computed using PCC in Equation 2. The belief b_v is considered as the trust score of user u on user v, i.e., $t_{u,v} = b_v$. M7 generates trust and distrust both via ratings. Distrust can be used in future for trust propagation.

8) M8: Bedi and Sharma [27] generate implicit trust scores from user-item rating matrix by combining similarity measure with confidence measure. Similarity is calculated using well known PCC.

$$sim_{u,v} = \begin{cases} P_{u,v} = \frac{\sum_i (r_{u,i} - \bar{r}_u)(r_{v,i} - \bar{r}_v)}{\sqrt{\sum_i (r_{u,i} - \bar{r}_u)^2} \sqrt{\sum_i (r_{v,i} - \bar{r}_v)^2}} \text{if } P_{u,v} > 0 \\ 0, \text{otherwise} \end{cases} \tag{14}$$

Confidence u should have in v is given as:

$$conf_{u,v} = \frac{|I_{u,v}|}{|I_u|} \tag{15}$$

Trust is calculated by performing Harmonic Mean of similarity and confidence.

$$t_{u,v} = \begin{cases} \frac{2 * sim_{u,v} * conf_{u,v}}{sim_{u,v} * conf_{u,v}}, & \text{if } sim_{u,v} \neq 0, conf_{u,v} \neq 0; \\ k * conf_{u,v}, & \text{if } sim_{u,v} = 0, conf_{u,v} \neq 0; \\ 0, & \text{if } sim_{u,v} = 0, conf_{u,v} = 0; \end{cases} \tag{16}$$

Here k is small constant. Since $conf_{u,v}$ may not be similar to $conf_{v,u}$ hence, the trust values generated are asymmetric. Ant colony algorithm is used for trust propagation and for promoting dynamic nature of trust. Although the metric is asymmetric and dynamic, but not context dependent.

B. Classification of Implicit Trust Metrics on The Basis of Trust Properties

Table 1 represents comparative analysis of eight implicit trust metrics, as discussed above, in terms of seven different trust properties with regard to TARS.

V. Discussion

In Table 1 eight different trust metrics are compared from the perspective of various trust properties with reference to TARS.

All the trust metrics (M1 to M8), fulfill transitivity property of trust. It is worth noting that, for metrics based on similarity measures, where similarity is computed using PCC (M2, M3, M7, M8), the PCC value need to be greater than 0.707, for metric to qualify the transitivity criteria.

TABLE I. Classification Of Trust Metrics On The Basis Of Trust Properties In Context To TARS

Trust Metric	Asymmetric	Transitive	Dynamic	Propagation	Network Perspective	Trust Establishment	Context Dependent
M1[19]	No	Yes	No	No	Local	Implicit	No
M2[22]	No	Yes	No	Yes	Local	Implicit	No
M3[26]	No	Yes	No	Yes	Local	Implicit	No
M4[18]	No	Yes	No	Yes	Local +Global	Implicit	No
M5[24]	No	Yes	No	Yes	Local	Implicit	No
M6[21]	No	Yes	No	No	Local	Implicit	No
M7[23]	No	Yes	No	No	Local	Implicit	No
M8[27]	Yes	Yes	Yes	Yes	Local	Implicit	No

Table 1 demonstrates that only metric M8 proposed by Bedi and Sharma, is asymmetric in nature. Rest of the trust metrics (M1-M7) are symmetric. M8 incorporates confidence measure along with similarity, which results it into an asymmetric metric.

Furthermore, metric M8 generates dynamic trust by updating trust values with time via ant colony optimization algorithm. Other trust metrics (M1-M7) does not support dynamic nature of trust. For generating dynamic trust it is suggested to incorporate evolutionary and genetic algorithms in the existing trust metrics.

None of the trust metrics has considered the context-dependency of trust into consideration. For context dependency, it is advisable to incorporate the contextual and behavioral information of users and items, in trust metrics, along with the normal item rating information.

Further, propagation of trust resolves the sparsity problem of traditional collaborative filtering. Hence, propagation is incorporated in majority of trust based RS [22], [26], [18], [24], [27].

Results in [18] have shown that global trust metric generates better rating coverage at the cost of prediction accuracy. However, global trust metric can be an effective solution for cold start users [27].

VI. Conclusion

This study presents a review of popular approaches in trust aware recommender systems, for implicit trust generation. The study also reviewed the definitions of trust along with computational properties of trust. Afterwards the explicit and implicit TARS architectures are examined, along with the limitations of explicit trust. Finally, eight different implicit trust metrics are reviewed and compared based on seven fundamental properties of trust in TRAS. From table-1 it is observed, that context-dependency have not received enough attention through the examined models and therefore new approaches are required, for incorporating the contextual property of trust in the trust metrics.

REFERENCES

[1] F. Ricci, L. Rokach, B. Shapira and P.B. Kantor, *Recommender Systems Handbook* , 2011.

[2] D. Goldberg, D. Nichols, B.M. Oki and D. Terry, *Using collaborative filtering to weave an information tapestry*, Commun ACM, vol. 35, no. 12, December, pp. 61-70.

[3] Hill, W., Stead, L., Rosenstein, M., and Furnas, G., *Recommending and evaluating choices in a virtual community of use*, In CHI 95: Proceedings of the SIGCHI conference on Human factors in computing systems, pages 194201, New York, NY, USA. ACM Press/Addison-Wesley Publishing Co.

[4] Shardanand, U.and Maes, P. (1995). , *Social information filtering: Algorithms for automating word of mouth"*, In Proceedings of ACM CHI 95 Conference on Human Factors in Computing Systems, volume 1, pages 210217.

[5] Resnick, P., Iacovou, N., Suchak, M., Bergstrom, P., and Riedl, J. (1994), *GroupLens: an open architecture for collaborative filtering of netnews*, In CSCW 94: Proceedings of the 1994 ACM conference on Computer Supported Cooperative Work, pages 175186, New York, NY, USA. ACM.

[6] Adomavicius, G. and Tuzhilin, A. (2005), *Toward the next generation of recommender systems: A survey of the state-of the- art and possible extensions*, IEEE Transactions on Knowledge and Data Engineering, 17(6):734749.

[7] Pazzani, M. J. and Billsus, D. (2007), *Content-based recommendation systems*, . In Brusilovsky, P., Kobsa, A., and Nejdl, W., editors, The Adaptive Web, Methods and Strategies of Web Personalization, volume 4321, pages 325341. Springer.

[8] McNee, S. M., Riedl, J., and Konstan, J. A. (2006), *Being accurate is not enough: how accuracy metrics have hurt recommender systems*, In Olson, G. M. and Jeffries, R., editors, CHI Extended Abstracts, pages 10971101. ACM.

[9] P. Massa and P. Avesani, *Trust-aware collaborative filtering for recommender systems*, In Proc. Of Federated Int. Conference On The Move to Meaningful Internet: CoopIS, DOA, ODBASE, 2004.

[10] J David Lewis and Andrew Weigert, *Trust as a social reality*, Social forces, 63(4):967985, 1985.

[11] Guibing Guo, Jie Zhang, Daniel Thalmann, Anirban Basu, and Neil Yorke-Smith,*From ratings to trust: an empirical study of implicit trust in recommender systems*, 2014.

[12] Stephen Paul Marsh, *Formalising trust as a computational concept*, 1994.

[13] Roger C Mayer, James H Davis, and F David Schoorman, *An integrative model of organizational trust*, Academy of management review, 20(3):709-734, 1995.

[14] A. Abdul-Rahman and S. Hailes, *Supporting trust in virtual communities*, In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS), 2000.

[15] J. Golbeck and J. Hendler, *Filmtrust: Movie recommendations using trust in web-based social networks*, In Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC), 2006.

[16] G. Guo, J. Zhang, and D. Thalmann, *A simple but effective method to incorporate trusted neighbors in recommender systems*, In Proceedings of the 20th International Conference on User Modeling, Adaptation and Personalization (UMAP), 2012.

[17] G. Guo, J. Zhang, and N. Yorke-Smith, *A novel Bayesian similarity measure for recommender systems* , In Proceedings of the 23rd International Joint Conference on Artificial Intelligence (IJCAI), 2013.

[18] C.-S. Hwang and Y.-P. Chen, *Using trust in collaborative filtering recommendation*, In New Trends in Applied Artificial Intelligence, 2007.

[19] N. Lathia, S. Hailes, and L. Capra, *Trust-based collaborative filtering*, In Trust Management II, 2008.

[20] P. Massa and P. Avesani, *Trust-aware recommender systems*, In Proceedings of the 2007 ACM Conference on Recommender Systems (RecSys), 2007.

[21] J. ODonovan and B. Smyth, *Trust in recommender systems*, In Proceedings of the 10th International Conference on Intelligent User Interfaces (IUI), 2005.

[22] M. Papagelis, D. Plexousakis, and T. Kutsuras, *Alleviating the sparsity problem of collaborative filtering using trust inferences*, In Trust management, 2005.

[23] G. Pitsilis and L. Marshall, *A model of trust derivation from evidence for use in recommendation systems*, Technical Report. University of Newcastle upon Tyne, 2004.

[24] Q. Shambour and J. Lu, *A trust-semantic fusion-based recommendation approach for e-business applications*, Decision Support Systems, 54:768780, 2012.

[25] A. Sotos, S. Vanhoof, W. Van Den Noortgate, and P. Onghena, *The transitivity misconception of pearson's correlation coefficient*, Statistics Education Research Journal, 8(2):33-55, 2009.

[26] W. Yuan, L. Shu, H. Chao, D. Guan, Y. Lee, and S. Lee, *itars: trust-aware recommender system using implicit trust networks*, Communications, IET, 4(14):17091721, 2010.

[27] Bedi, Punam and Ravish Sharma, *Trust based Recommender System using Ant Colony for Trust Computation*, Expert Systems with Applications. 39(1): 11831190. Elsevier (Impact factor 2.203, 5-year impact factor 2.455), 2012.

[28] Swati Gupta, Sushama Nagpal *An Empirical Analysis of Implicit Trust Metrics In Recommender Systems*, ICAIS 2015, (accepted for forthcoming conference in Aug, 2015).

[29] K. Dyczkowski, A. Stachowiak, *A Recommender System with Uncertainty on the Example of Political Elections*, Advances in Computational Intelligence, Communications in Computer and Information Science, vol 298, pp. 441- 449, Springer, Berlin Heidelberg, 2012.

[30] A. Stachowiak, *Uncertainty-Preserving Trust Prediction in Social Networks*, Social Networks: A Framework of Computational Intelligence, pp. 99-122, Springer, 2014.