Soc. Netw. Anal. Min. (2013) 3:65–84
DOI 10.1007/s13278-012-0049-9

ORIGINAL ARTICLE

Pruning trust–distrust network via reliability and risk estimates for quality recommendations

Deepa Anand · K. K. Bharadwaj

Received: 25 May 2011 / Revised: 9 December 2011 / Accepted: 13 January 2012 / Published online: 4 February 2012

Abstract The efficacy of trust links from social networks in boosting the user inter-connectivity in an otherwise poorly connected user group, obtained from historical preference data, has recently led to adoption of systems exploiting both these information sources to discover user proximities for recommender systems (RS). However, the investigation into the utility of distrust in the recommendation process is in its infancy. We propose a collaborative filtering framework based on computing user trust by exploiting functional and referral trust and distrust information together with user preference data. The inclusion of multiple sources of opinions for computing trust results in improved coverage and the trust network so formed can be used to infer indirect trust between entities by exploiting transitivity of trust. We also quantify the risk in relying on trust statements as a function of knowledge contained in the statement and the conflict in opinions about an entity and argue that pruning the trust graph by discarding risky and retaining reliable trust statements results in more accurate and robust recommendations while not compromising on the coverage. The experimental results corroborate our ideas and outperform several baseline algorithms.

Keywords Web personalization · Recommender systems · Collaborative filtering · Trust and distrust · Social networks

D. Anand (✉)
CMR Institute of Management Studies, No. 2, 3rd 'C' Cross, 6th 'A' Main, 2nd Block HRBR Layout, Bangalore 560043, Karnataka, India
e-mail: deepanand209@gmail.com

K. K. Bharadwaj
School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi 110067, India
e-mail: kbharadwaj@gmail.com

1 Introduction

The sparseness of user-expressed preference information deters reliable similarity estimates in collaborative filtering. The presence of additional information in the form of contents details (Zhao et al. 2010; Kayaalp et al. 2011), tags (Cantador et al. 2010; Hamouda and Wanas 2011) or trust (Dell'Amico and Capra 2008; Liu and Yuan 2010) have been harnessed to supplement the set of user connections and ease of information exchange. In particular, the growing popularity of social networks and the wealth of interpersonal relationships inferable from them have resulted in the utilization of these social links to extend the number of users who can collaborate. In fact both recommender systems (Burke 2002; Chen and Qi 2011) and social networks are mediums through which users can interchange useful information and have been used in the past to aid each other. Recommendation algorithms can be used to search for potential friends and social network links can be used to form relationships between users not sharing any co-rated items. This bidirectional effect of trust and rating has been demonstrated in Matsuo and Yamamoto (2009) and shows a strong correlation between the two quantities, i.e., the preference information of a user's trusted neighbors strongly matches with his preferences and tastes.

Though there has been a wealth of work on combining trust networks and recommender systems, distrust has by far been a little explored solution for RS mainly due to the dearth of freely available datasets consisting of trust, distrust and rating information. Another reason for this is that earlier approaches (Prade 2007; Golbeck et al. 2003) viewed trust and distrust as two ends of a continuum, and were represented along a single dimension with distrustworthy parties conferred a trust value of 0 and trusted

parties having a trust value of 1. The absence of distrust as a separate dimension in prior work renders the modeling and propagation of distrust unclear. As an example if an entity 'A' seeks an opinion about another entity say 'B' from two of its trusted neighbors say 'C' and 'D'. C might distrust 'B' and so give a trust value of 0. 'D' not being familiar with 'B' might not be able to evaluate his trustworthiness and thus again assign a trust value of 0. 'A' in this case is unable to differentiate between distrust (C) and ignorance (D). Thus, recent research has revealed the existence of trust and distrust along different dimensions (Victor 2010; Guha et al. 2004) and that both can separately reveal the pattern of user relationships. Both user rating data and friend/block list information from social networks are very sparse. This is so since any user can rate only a limited subset of items or users from among the millions of ratable items/users and hence the idea of combining these information sources is promising and justifiable. We propose a collaborative filtering framework which operates on a trust network where the trust relationship has three components namely, trust, distrust and ignorance (Yu et al. 2008). To demonstrate the effectiveness of our ideas we perform experiments on data extracted from Epinions which is one of the few datasets which incorporate user preferences and trust and distrust information. However, the trust and distrust information expressed in Epinions is binary and thus fails to express the social tie strength. We thus propose to construct a trust network based on user-expressed preferences for items and his friends/block list. This has the advantage of grading various entities according to their trustworthiness thus giving rise to continuous trust and distrust values in addition to enhancing the link density in the network. Previous work have harnessed other information sources such as tags, item content (Liu and Yuan 2010) and navigational patterns (Esslimani et al. 2010) in addition to user-item ratings data for boosting user connectivity for enhanced recommendations. The proposed method of trust network construction relies only on trust and item ratings by the user and differs from previous approaches by using a referral trust and distrust component in addition to explicitly expressed trust–distrust statements and item ratings. The trust network so constructed is then mined to form opinions amongst users who have never interacted before, by employing trust propagation and aggregation operators.

However, when concluding about the trustworthiness of an entity through common experiences, with respect to users or items, a certain amount of precaution is essential. When the trust and distrust assessment is based on a handful of common experiences or an almost equal number of favorable and unfavorable experiences then utilizing the trust measure so derived may not only lead us to incorrectly judge a person as trust or distrustworthy, but also may impact the kind of users reachable through them via trust transitivity. This is in accordance with our day-to-day practice of not heeding to opinions from peers with whom we have not interacted much or about loyalties of those we are undecided. We thus propose several risk assessment policies to compute the risk or reliability of trust statements inferred and investigate how such judgments aid in improving the quality of links in the trust networks. Once the statements are assessed for their reliability the highly risky ones are removed from the network or scaled down and the modified network so obtained is utilized to infer indirect trust through trust propagation and aggregation. Though previous work has explored the strength or weakness of social ties in deciding their influence for various tasks (such as recommendations), the reliability of inferred trust and distrust as a pruning criteria, especially in a network incorporating both trust and distrust degrees has not been proposed previously.

The remainder of the paper is structured as follows. Section 2 presents the related work. Section 3 discusses strategies for constructing the trust network and describes the trust propagation and aggregation techniques used. Various risk assessment policies are described in Sect. 4. Section 5 presents the experimental setup and results which establish the superiority of the proposed ideas over baselines. We discuss the conclusions and point out direction for future work in Sect. 6.

2 Related work

The rapid expansion of Web 2.0 has given rise to several applications involving social networks linking users and enabling them to produce content, which can be mined to deduce user interconnections. These connections in turn help in enhancing and customizing web content for users by exploiting the preferences of like minded users deduced from the connections. In this section we describe several techniques through which social networks are used to enrich user web experience through personalization. Thereafter, trust and distrust propagation and aggregation operators from the existing literature are discussed and we conclude with the various interpretations of risk and its relation to trust under various contexts.

2.1 Collaborative filtering and trust networks

Collaborative filtering systems (Adomavicius and Tuzhilin 2005; Anand and Bharadwaj 2010b) are based on cooperation amongst a community of users to garner opinions about various unencountered items. To decide on the people from whom opinions are sought, the affinity

between users is gauged and votes from users having similar preferences are analyzed to decide on the likeability of items for the active user. CF systems are generally categorized into memory-based and model-based systems (Breese et al. 1998). While memory-based algorithms utilize the entire rating history to make predictions, model-based systems (Al-Shamri and Bharadwaj 2008; Bell et al. 2007) build a user model and base their recommendations on it. Memory-based algorithms typically treat the set of item ratings by each user as a vector and assess the similarity between users by comparing rating vectors. Pearson correlation coefficient (Resnick et al. 1994) and vector similarity (Breese et al. 1998) are two of the most popular similarity measures used.

Though the virtual bonds inferred between users, by utilizing preferences expressed explicitly or implicitly by them, facilitate collaboration, it is hindered by the scarcity of sufficient number of links in general, since for many user pairs the bonds are not deducible. This sparsity problem (Anand and Bharadwaj 2010a), which poses a major challenge to recommender systems, can be resolved by utilizing additional data like item features, tagging information, etc. to find connections between users or items. However, with the ability to create our friend/block list in many of the web-based applications, the explicitly specified trustworthy or distrustworthy user information can be harnessed to help in the CF process.

Trust-based approaches to CF can be broadly classified into methods which deduce the trust ranking based on ratings data alone, due to the nonexistence of explicit trust votes (Pitsilis and Knapskog 2009; Bharadwaj and Al-Shamri 2009) and others such as Golbeck's TidalTrust algorithm (Golbeck 2005) and MoleTrust (Massa and Avesani 2007) which rely on similarity estimate only based on the trust network available. Estimation of user similarity based on ratings alone makes the system susceptible to misleading recommendations (Dell'Amico and Capra 2008), but on the other hand relying only on trusted users may lead to poor results if the user though well intentioned is a poor recommender. SOFIA (Dell'Amico and Capra 2008) is a recommendation algorithm which evaluates a user on his 'intention' and 'competence' and aims at seeking recommenders who are reasonably well intentioned as well as competent. Such an evaluation is performed based on trust and ratings data. Konstas et al. (2009) developed a track recommender systems based on data derived from a popular internet radio site, last.fm, interlinking tags, user and items and the interrelations among the three entities are exploited to form links between users. The extra knowledge provided by the user's social activity was shown to improve system performance using Random Walk with Restart. A number of similar approaches (Jamali and Ester 2009; Liu and Yuan 2010) aim to supplement user links deducible through ratings data through other information sources. Though the inclusion of such varied information sources comes handy in improving user connectivity, they require content details about the items which may be difficult to come by in certain domains. A new approach, densified behavioral network CF(D-BNCF) (Esslimani et al. 2010), exploits navigational patterns, instead of the ratings or social connections, to establish user similarity through a behavioral network. The network so constructed is densified by exploiting link prediction methods to enhance the user links. The D-BNCF approach is similar to the proposed approach since both attempts to enhance the existing user network with additional links. But D-BNCF approach only exploits the usage traces to construct the initial network, whereas the current approach exploits the availability of trust and ratings data to construct the initial user graph. Another point of difference is that though D-BNCF only considers similar navigational and connectivity patterns to infer similarity, the proposed approach models both the similar and dissimilar experiences between users as trust and distrust and is hence able to capture the user connections more vividly.

The availability of the information regarding the set of peers distrusted by users, has recently led to the emergence of algorithms exploiting this additional source to refine the user links. Victor et al. (2009a, b) detail a scheme of trust assessment between unconnected parties in a trust network by using trust propagation and aggregation operators and explore various ways in which distrust information can be utilized to fine-tune such a network. A friend recommender system in online social networks utilizes the FriendTNS (Symeonidis et al. 2010) algorithm to transitively assess user trustworthiness in the presence of positive as well as negative edges. Though the incorporation of distrust in addition to trust for improved recommendations has been previously dealt with, to the best of our knowledge, derivation of trust and distrust degree from the existing trust, ratings and referral trust data has not been explored before. Such estimation of trust and distrust degrees from the available data has several advantages. It allows representation of trustworthiness of an entity as a continuous value with some amount of trust and distrust as opposed to complete trust or distrust. This corresponds with our day-to-day experiences where the strength of our friendship links may vary from person to person and many a times we may harbor some amount of like as well as dislike for a person. Secondly, the incorporation of referral trust in the final trust and distrust computation renders the values useful for referrals in addition to

recommendations and thus justifies trust transitivity. And lastly, the trust network so obtained is denser than the original trust network thus allowing more users to be connected.

2.2 Inferring indirect trust and distrust

Trust information in addition to being an explicitly specified link between users is also very useful since transitivity of trust can be utilized to further expand the user neighborhood. There have been several schemes proposed in literature to infer indirect trust through the trust network. Golbeck's TidalTrust algorithm (Golbeck 2005) uses weighted average of the degree of trust on a distant entity obtained from the neighbors, to recursively compute the trustworthiness of a user from another's standpoint, based on the paths that connect them in the network and the trust ratings on those paths. A similar standpoint is taken in MoleTrust (Massa and Avesani 2007) which operates by performing a breadth first search of the trust graph in order to find shortest paths to all users within a predefined trust propagation horizon. The degree of trust from the active user to the other users is computed on a level-by-level basis so that the trust on a user at a level '*L*' is formulated as a function of trust on users at level '*L-1*'. Wang and Singh (2010), presents an evidence-based account of trust where a mapping from evidence space to trust is established based on certainty. The certainty in turn is modeled on conflict in the evidence.

Guha et al. (2004) were one of the first ones to propose propagation schemes in the presence of trust and distrust. They suggested four basic trust propagation schemes namely transitivity, trust coupling, reciprocity and co-citation. They propose a framework utilizing both trust and distrust information to infer trust between unfamiliar users. Propagation of distrust also has harnessed in tackling the web spamming problem (Wu et al. 2006; Metaxas 2009) and combining trust and distrust has proven to be more effective in demoting spam sites than the sole application of trust for this purpose. Victor et al. (2009a, b) also suggest several strategies for inferring indirect trust in the presence of trust and distrust links in the network, which are based on various user behaviors when confronted with situations in which they collate opinions about strangers from friends or foes. They argue that trust or distrust building is a gradual process where an encounter between a pair of entities can give rise to some amount of trust as well as distrust on the entity and operate on trust, distrust pairs drawn from a bilattice.

Dempster Schaffer (DS) theory has been the basis of several techniques of trust and distrust assessment since it allows the embedding of uncertainty in the derivation process and one of the prominent work in this direction has been done by Jøsang et al. (2006a, b). Subjective logic framework, which is based on DS theory, has been proposed to reason with trust information. The trustworthiness information is expressed as a four tuple (trust, distrust, uncertainity, base rate) and the trust network is simplified by expressing it in canonical form to deduce the indirect degree of trust in a distant entity. Another popular contribution by Yu and Singh (2002) where an agent combines evidence from direct interactions with testimonies provided by other users regarding the same agent with the help of DS theory, has spawned other extensions (Matt et al. 2010; Qiu et al. 2010). Gutscher (2009) contend that the DS theory is inadequate when combining conflicting evidence since it eliminates the conflict by renormalization. Hence, they propose to represent the trustworthiness information as a four tuple (trust, distrust, ignorance, conflict) and develop a calculus and operators to compute reputation values. A similar argument is put forth in Wang and Sun (2009) where DSmT belief theory, which is an extension of DS theory and which explicitly quantifies the conflict in evidence, is used to model trust information.

2.3 Trust and risk

Among the various human factors impinging upon making a decision in an uncertain environment, risk and trust are surely crucial ones (Jøsang and Lo Presti 2004). Delegation of tasks, such as recommendations, on trusted peers naturally incurs the risk of unfavorable results when the trustee is unable to perform the task satisfactorily. Thus, trust and risk are highly correlated concepts and their relationship has been extensively investigated in literature. Several articles analyze the relationship between trust and risk and lay forth computational models integrating the two notions (Gambetta 2000; Jøsang and Lo Presti 2004) They model the trusting decision as a function of trustworthiness of a user and the risk attitudes of the trustor. Techniques for trust and risk propagation have also been studied in Gray et al. (2003), Lin et al. (2008).

The notion of risk as defined in this work, however, deviates from the previous interpretations and quantifications of risk on several points. We define risk as a measure of lack of reliability on the evidential trust and distrust values inferred rather than the risk of interacting with an entity. Whereas previous work view risk as a dimension separate from trust, the risk measure defined in our approach depends on the trust and distrust values. A low-risk trust statement thus inspires more confidence on the trust–distrust values deduced. We examine various risk assessment policies and their relation to trust and distrust in greater detail in Sect. 3.

2.4 Attacks on collaborative filtering systems

Since CF systems are social systems which rely on inputs from a large user set, they have been subject to abuse by malicious behaviors: for example, malicious users could copy honest users' reviews, to gain high similarity scores with them; they could subsequently inject inflated reviews in the system, to trick those users into buying an item or, vice versa, to disrupt an item's sales (Dell'Amico and Capra 2008). The ease of creating identities in most of the web-enabled systems enables attackers to create multiple fake profiles in order to influence the ratings for the particular items. Such attacks, called shilling attacks, can be categorized into push attacks, which artificially enhance the rating of an item, or nuke attack, which attempt to downgrade the popularity of an item. Mobasher et al. (2007) proposed several attack models and their effects on recommendations. In a shilling attack the fake user profile is divided into four parts: a singleton target item (to be pushed or nuked), a set of selected items for which ratings are assigned depending on the attacker's intent, a set of filler items for which ratings are assigned at random and a set of unrated items. Based on the attack profile several attack models have been proposed in literature but the aim of this article is to examine the effects of four attack models as described below, on the system.

- *Random attack* Ratings around the system average are randomly assigned to the filler item set and the selected item set is empty.
- *Average attack* Items in the filler set are assigned ratings drawn from the rating distribution for the item.
- *Bandwagon attack* A few very popular movies are chosen as the selected items and are assigned high ratings. This enables the attack profile to match with several users who may also have assigned high ratings for the popular movies. The filler items are assigned random ratings.
- *Reverse bandwagon* This attack associates the target item, with a set of widely disliked items, by assigning it the lowest rating, to nuke that item. This will increase the probability that the system will generate low predicted ratings for it.

Random and average attack profiles may assign the target item the highest or lowest rating depending on whether the item needs to be pushed or nuked. One of the most effective solutions to the attack on CF systems is to use explicitly specified trust judgments to filter out the influence of potential fake profiles. However, only using explicit trust judgments to select similar users may impact the number of recommendations possible (coverage) as well as the accuracy, since some users though well intentioned may not have similar tastes as the active user. In this paper, we investigate the combined approach to using trust, distrust and ratings for its ability to enhance accuracy and coverage as well as in its ability to deflect attacks.

3 Proposed framework

This section describes our trust representation scheme and put forth our technique of enhancing the existing trust network by appending edges based on the preference and referral information. We demonstrate the advantage offered by the trust network so populated in enhancing recommendation quality in Sect. 5.

3.1 Trust representation

Trust has been increasingly used in the area of recommender systems (RS) as a means to enhancing recommendation accuracy by leveraging on the inputs from trusted users. In addition to trust relationships, deduced from the friends list, the distrust information (users in the block list, for example) is also being utilized to protect parties from the risk of being exploited by malicious parties by barring such distrust worthy users from contributing towards recommendations. We compute the measure of trust and distrust worthiness of a user from another's point of view not only based on the explicitly specified friend/block list but also from the experiences shared by the pair of users. When employing such evidential approach to building a trust network, the fact that there may be several pairs of users who may be unaware of each other or may not have had a variety of common experiences, is worth considering. Hence, the modeling the trust relationship between such users would require the specification of uncertainty or ignorance. We wish to model trust information on belief theory as originally proposed by Dempster–Shafer (Shafer 1976). Their theory is based on a frame of discernment θ which in our case would be $\{T, \sim T\}$. These are the set of propositions under consideration.

Def 1: Let $\ominus$ be a frame of discernment. A basic belief assignment (bba) is a function m:$2^{\ominus} \rightarrow [0,1]$ such that $m(\phi) = 0$ and $\sum_{A \subseteq \theta} m(A) = 1$.

The main idea behind belief theory is to abandon the additivity principle of probability theory and enable observers to assign the so-called belief mass to any frame of discernment including the whole frame itself. This facilitates representation of uncertainty or ignorance by assigning a belief mass to the whole frame (Jøsang et al. 2010). Hence for the frame of discernment $\theta = \{T, \sim T\}$, $m(T)$, $m(\sim T)$ and $m(\{T, \sim T\})$ denote the trust, distrust and the ignorance, respectively, and so

$$m(T) + m(\sim T) + m(\{T, \sim T\}) = 1 \quad (1)$$

$m(T)$, $m(\sim T)$ and $m(\{T, \sim T\})$ would henceforth be referred to by t(trust), d(distrust) and i(ignorance), respectively. Equation 2 can be re written as

$$t + d + i = 1. \quad (2)$$

Since the amount of ignorance can be derived from trust and distrust information, we denote the trust relation between a pair of users by the trust and distrust pair, i.e.

$$T(A, B) = (t, d)$$

where $T(A,B)$ is the trust opinion of A about B.

3.2 Populating the extended trust network (ETN)

We assume a system with a set of users $U = \{u_1, u_2, \ldots, u_m\}$ and a set of items $I = \{i_1, i_2, \ldots, i_n\}$. The trust network we operate on is constructed by appending edges from user A to B, to the network, if either of the options below holds.

1. If A and B share common experiences (have rated common items) (*Trust and Distrust by preference matching*—($T_P(A,B)$, $D_P(A,B)$)).
2. If A and B have rated a common set of users on trust (*Referral Trust* and *Referral Distrust* T_R (A,B), D_R (A,B)).
3. If A has expressed his trust/distrust in user B (*Direct Trust and Direct Distrust* ($T_D(A,B)$, $D_D(A,B)$)).

We model the final trust/distrust degrees as a linear combination of trust/distrust degrees derivable from the above-mentioned information sources, i.e.

$$\begin{aligned} t &= \alpha T_p(A,B) + \beta T_R(A,B) + \gamma T_D(A,B) \\ d &= \alpha D_p(A,B) + \beta D_R(A,B) + \gamma D_D(A,B) \end{aligned} \quad (3)$$

where $\alpha + \beta + \gamma = 1$. Here α, β and γ are parameters that represent the influence of the trust–distrust components derived from preference matching, referral trust–distrust and explicitly specified trust–distrust rating, respectively, when combining the components linearly.

In the formula (3) above T_D and D_D are degrees of trust and distrust worthiness expressed explicitly by A about B and thus are readily available. To compute (T_P, D_P), we exploit the existing item preference information available in the form of user voting data. An item is reckoned to be preferred by a user if its vote is higher than the vote that the user confers on items on an average and similarly is disliked by the user if its rating is below the average ratings by the user. If the rating is, however, equal to the average then no decision about its likeability can be made. Thus, the preference of an item I for user A is defined as:

$$\text{Preference}(A, I) = \begin{cases} 1, & \text{if rat}(A,I) > \text{mean}(A) \\ 0, & \text{if rat}(A,I) = \text{mean}(A) \\ -1, & \text{if rat}(A,I) < \text{mean}(A) \end{cases} \quad (4)$$

where *rat(A,I)* is the rating value for item I by user A and *mean(A)* is the average user rating for A.

Here a value of -1 is an indicator of A's disfavor to I. To compute the trustworthiness of B from A's point of view, for each common item experienced by A, the preference of the item, if experienced by B, is matched with that of A. The trust and distrust are then computed as the fraction of matches and mismatches. Assuming that $L^i(A)$ and $DL^i(A)$, respectively, represent the set of items liked and disliked by the user A, $T_P'(A,B)$ and $D_P'(A,B)$are defined as:

$$\begin{aligned} T_P'(A,B) &= \frac{1}{2}\left[\frac{|L^i(A) \cap L^i(B)|}{|L^i(A)|} + \frac{|DL^i(A) \cap DL^i(B)|}{|DL^i(A)|}\right] \\ D_P'(A,B) &= \frac{1}{2}\left[\frac{|L^i(A) \cap DL^i(B)|}{|L^i(A)|} + \frac{|DL^i(A) \cap L^i(B)|}{|DL^i(A)|}\right] \end{aligned} \quad (5)$$

where $L^i(A) = \{k \in I \,|\, \text{Preference}(A,k) = 1\}$ and $DL^i(A) = \{k \in I \,|\, \text{Preference}(A,k) = -1\}$. Thus, the fraction of items for which the opinions of A and B matched contribute to the trust and by extension the set of items for which there was a clash of opinions is indicative of the amount of distrust that A harbors against B. Note that since the fraction is computed against the number of items liked and disliked by A such a computation of trust and distrust makes the quantities asymmetric which is in sync with our notion of trust and distrust in our day-to-day life. However, the above formulae work only if A's set of experienced items is substantial enough, since computations based on a small number of experiences is not reliable. To overcome this hitch we extend the formulae to scale down the trust and distrust degrees if the set of items liked or disliked by the user is smaller than a predetermined set size denoted by δ. Hence the formulae (5) extends to

$$\begin{aligned} T_P(A,B) &= \frac{1}{2}\left[\frac{\min(\delta, |L^i(A)|)}{\delta} \times \frac{|L^i(A) \cap L^i(B)|}{|L^i(A)|} \right. \\ &\quad \left. + \frac{\min(\delta, |DL^i(A)|)}{\delta} \times \frac{|DL^i(A) \cap DL^i(B)|}{|DL^i(A)|}\right] \\ D_P(A,B) &= \frac{1}{2}\left[\frac{\min(\delta, |L^i(A)|)}{\delta} \times \frac{|L^i(A) \cap DL^i(B)|}{|L^i(A)|} \right. \\ &\quad \left. + \frac{\min(\delta, |DL^i(A)|)}{\delta} \times \frac{|DL^i(A) \cap L^i(B)|}{|DL^i(A)|}\right] \end{aligned} \quad (6)$$

It is to be noted that the lack of sufficient experienced items results in reduced trust and distrust degrees but in turn results in more uncertainty or ignorance which is as is expected.

The referral trust and distrust can be computed in a similar fashion since here the ratings are for users instead of items. We assume a system where the trust elicitation is binary, i.e., users express other users as trustworthy or distrustworthy but do not specify the amount of trust or distrust. We thus arrive at the formulae for computing trust distrust through referrals, (T_R,D_R) by following the same argument as for trust and distrust through preferences, (T_P,D_P) as:

$$\begin{aligned} T_R(A,B) &= \frac{1}{2}\left[\frac{\min(\rho,|L^u(A)|)}{\rho}\times\frac{|L^u(A)\cap L^u(B)|}{|L^u(A)|}\right. \\ &\quad \left.+\frac{\min(\rho,|DL^u(A)|)}{\rho}\times\frac{|DL^u(A)\cap DL^u(B)|}{|DL^u(A)|}\right] \\ D_R(A,B) &= \frac{1}{2}\left[\frac{\min(\rho,|L^u(A)|)}{\rho}\times\frac{|L^u(A)\cap DL^u(B)|}{|L^u(A)|}\right. \\ &\quad \left.+\frac{\min(\rho,|DL^u(A)|)}{\rho}\times\frac{|DL^u(A)\cap L^u(B)|}{|DL^u(A)|}\right] \end{aligned} \tag{7}$$

where $L^u(A)$ is the set of users that A deems trustworthy, $DL^u(A)$ is the set of distrustworthy users for A and ρ is the predetermined set size to ensure the minimum experience needed by the user in expressing his like or dislike of other users.

Once the trust and distrust worthiness of B is evaluated by A along the three dimensions namely, direct, preference based and referral, the final trust and distrust between the entities can be computed as given in formula (3) and the recommendation technique utilizing the network so obtained shall henceforth be referred to as extended trust network (ETN). The ETN so constructed can then be analyzed to connect more users by exploiting the general user tendency to place some amount of trust on the friend of a friend. The method employed to infer such indirect trust and distrust is detailed in the next subsection.

3.3 Indirect trust derivation

Several techniques to deduce the trust relationship between unconnected users in a trust network have been analyzed and evaluated in literature and Sect. 2 provides a review some of the popular approaches. When a user, say A, does not have a direct trust connection with another user, say B, but wishes to assess his trustworthiness he usually seeks out a connection to B through his trusted neighbors. The trust evaluation along a path in a trust network from one user to the other is done through trust concatenation or propagation. When several paths to the target user exists via various trusted neighbors of A, then the resultant indirect trust from various sources need to be combined and this is termed trust fusion or aggregation. Evaluation of distant entities in a trust network is usually done by enumerating the paths between the two users, say A and B, and applying concatenation and fusion to arrive at indirect trust scores.

There has been a wealth of research which has gone into effective fusion of beliefs and has been utilized to reason about the trust or distrust worthiness of individuals. Dempster's rule is one of the very well researched rules for belief fusion and has been adopted by Yu and Singh (2002) for trust evaluation of objects from a user's point of view. The inability of DS theory in handling completely conflicting evidence and the counter-intuitive results produced under high conflict has been documented and has given rise to several extensions. Wang and Sun (2009) propose to reason with trust and distrust using an extension to DS theory which is called the Dezert–Smarandache theory (DSmT) and which relaxes the exclusivity condition of the events in the frame of discernment. Thus, conflicting situations are handled by allowing a belief mass to be assigned to the set $\{T \cap \sim T\}$ where the frame of discernment is $\theta = \{T, \sim T\}$. Gutscher (2009) also extends tri-component trust representation using DS theory and augments it with a new parameter 'conflict' and develops the calculus and operators to combine beliefs under this new representation. Though Gutscher (2009) and Wang and Sun (2009) are able to handle conflict in opinions while combining beliefs they suffer from a drawback as illustrated by the following example.

Example 1 Suppose a user A seeks opinions from its trusted set of users about another user B with whom A has no interactions. As shown in Fig. 1a, the trusted neighborhood of A consists of three users C, D, and E. Here C and D trust B, whereas E distrusts B. Combining the opinions from C, D, and E using Dempster's rule would not be possible, whereas Gutscher (2009) and (Wang and Sun (2009) would conclude total conflict with trust, distrust and ignorance computed as 0, as they ignore the quantity of opinions expressed for and against trusting a user when inferring trust on a distant entity. In fact any number of positive opinions about a distant user can lead to a total conflict by the introduction of just one distrust statement. Intuitively though there does exist a conflict in the opinions, the balance is slightly tilted towards trusting B albeit with a degree of distrust as well.

Figure 1b shows the opinions gathered by A about B through his trusted neighbors C, D and E. The edges are shown in gray since these are indirect views. A simple

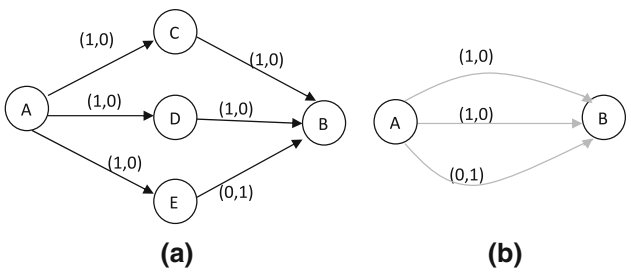

Fig. 1 **a** Portion of trust network connecting users A and B. **b** A's opinions about B inferred from C, D, E

average of the trust statements (average of the individual components) would lead to a more intuitive result, i.e. $T(A,B) = (0.66,\ 0.33)$. There is some conflict when the results are aggregated which is indicated by the amount of trust and distrust degrees being nonzero, but the trust degree is higher since more people have expressed B as trustworthy.

We argue that when deducing trust relationship based on evidential information the degrees of trust and distrust are themselves good indicators of the conflict. The closer these quantities are to each other the higher is the conflict in opinions. Thus, we prefer aggregation operators having the desirable property of factoring in the quality as well as quantity of trust versus distrust opinions and choose to apply the cumulative fusion operator as proposed in Jøsang et al. (2010).

Def Cumulative Fusion Rule (Jøsang et al. 2010): Let m_A and m_B be two **bba**s, respectively, by agents A and B over the same frame of discernment θ. Let the power set of θ be $X = \{x_i : i = 1, \ldots, n\}$. Then the cumulatively fused belief m_{AoB} is defined as:

$$\frac{\text{CaseI} : \text{For}\, m_A(\theta) \neq 0 \ \vee \ m_B(\theta) \neq 0}{\begin{cases} m_{AoB}(x_i) = \frac{m_A(x_i)m_B(\theta) + m_A(\theta)m_B(x_i)}{m_A(\theta)+m_B(\theta)-m_A(\theta)m_B(\theta)} \\ m_{AoB}(\theta) = \frac{m_A(\theta)m_B(\theta)}{m_A(\theta)+m_B(\theta)-m_A(\theta)m_B(\theta)} \end{cases}} \tag{8}$$

$$\frac{\text{Case II} : \text{For}\, m_A(\theta) \neq 0 \ \wedge \ m_B(\theta) \neq 0}{\begin{cases} m_{AoB}(x_i) = \gamma^A m_A(x_i) + \gamma^B m_B(x_i) \\ m_{AoB}(\theta) = 0 \end{cases} \text{where} \begin{cases} \gamma^A = \lim\limits_{\substack{m_A(\theta)\to 0 \\ m_B(\theta)\to 0}} \frac{m_B(\theta)}{m_A(\theta)+m_B(\theta)} \\ \gamma^B = \lim\limits_{\substack{m_A(\theta)\to 0 \\ m_B(\theta)\to 0}} \frac{m_A(\theta)}{m_A(\theta)+m_B(\theta)} \end{cases}}$$

This fusion process incorporates ignorance in weighing the two opinions. The higher the ignorance the lesser the influence of the corresponding trust or distrust value in the final trust or distrust value. The cumulative fusion operator is non-idempotent, and this non-idempotence can be leveraged to strengthen beliefs while combining it with similar beliefs, as illustrated with an example in Jøsang et al. (2010). The choice of cumulative fusion operator for trust aggregation, is based on its ability to

1. Take into consideration the number of opinions supporting or opposing the trust in an entity.
2. Leverage its non-idempotence to strengthen beliefs which are close to each other and decrease the ignorance as the number of inputs increase.

For trust propagation we use "Opposite Belief favoring" (Jøsang et al. 2006a, b) where A's disbelief in another user B means that A thinks that B consistently errs in his judgments. Hence computation of trust values from A to C where A is connected to C via its trusted neighbor B (Fig. 2), is as computed as

$$t(A,C) = (t1 \times t2 + d1 \times d2,\ \ t1 \times d2 + d1 \times t2) \tag{9}$$

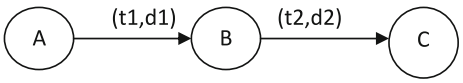

Fig. 2 Trust propagation: Opposite belief Favoring (Jøsang et al. 2006a, b)

The above-discussed trust propagation operators when applied to the proposed ETN aids in establishing previously unknown relationships among users and this in turn helps in improving collaboration among users. This technique would henceforth be referred to as trust propagation in extended trust network (TP-ETN).

4 Trust network pruning

The explicitly specified trust relation between a pair of users, in general, does not consist of both a degree of trust and distrust. Rather users generally specify another as trustworthy or non trustworthy albeit with degrees of trust or distrust worthiness (e.g., Apprentice, Journeyer, and Master, advogato.org/trust-metric.html). However, when considering indirect evidence to determine trust relation between a pair of users or when combining opinions about the same user from different sources, we may obtain evidence both supporting and opposing the trust and distrust worthiness of a user in varying degrees. Given the trust relationship between two users X and Y, $T(X,Y) = (t,d)$, the decision about whether Y is trustworthy or distrustworthy is determined by comparing the evidence for and against trusting him. If $t > d$ then Y is considered trustworthy and if $t < d$ then he is considered distrustworthy. An evaluation of the trustworthiness of a user with t and d equal renders such an evaluation useless, since the user cannot be concluded to be trust or distrust worthy. Thus, given any $T(X,Y) = (t,d)$, if $t > d$ then the hypothesis '*X trusts Y*' holds true with degree of support t and degree of refutation d. Similarly when $t < d$ then the hypothesis '*X distrusts Y*' holds with degree of support d and degree of refutation t. The degree of trust or distrust worthiness is generally obtained as the difference in the degree of trust and distrust($|\ t - d\ |$) (Guha et al. 2004).

4.1 Risk evaluation strategies

The computation of trust and distrust degree, as described above, may have an associated risk involved. For example a trust relationship between X and Y with $T(X,Y) = (0.2,\ 0.1)$ allows us to conclude that Y is trustworthy and degree of trust is **0.1**. However, this trust assessment may not be very dependable since the ignorance is high and hence such an assessment is based on very little knowledge thus rendering it risky. The risk arises since with more evidence

coming in it is possible that the situation changes drastically, say increasing the distrust degree more than the trust, and hence making the previous judgment erroneous by deeming a distrustworthy party to be trustworthy.

Consider another situation with two trust assessments *T1* and *T2* such that $T1(X,Y) = (0.5, 0.3)$ and $T2(X,Y) = (0.2, 0)$. Though both conclude that *Y* is trustworthy and the trust degree is *0.2*, there can be different arguments with regards to the dependability of *T1* and *T2*.

Argument 1: *T1* is less risk prone since it is based on less ignorance and hence on more trust, distrust provenance information.

Argument 2: *T2* is more dependable since there is no reason to distrust *Y* and thus no refuting evidence.

As the above examples illustrate there may be an inherent risk in concluding about the trust or distrust worthiness of users when both trust and distrust measures are present. Quantifying the risk involved in judgment of trust and distrust may aid in choosing more dependable trust relationships for assessing the trustworthiness as well for trust propagation. Evaluation of trustworthiness based on dependability is expected to result in better quality trusted neighborhood thus effectively bettering the recommendation quality. As seen in both the examples above ignorance is one of the deterrents to dependable trust assessment. A trust assessment is risky if there is a high chance of an erroneous judgment as to the trustworthiness of the person, i.e. a trustworthy person is adjudged distrustworthy or vice versa. The less the risk associated with a trust statement the more dependable it is. Moreover, trust statements which are supported and refuted almost equally are also more prone to risk due to the high conflict. In Example 2 above though *T1* is based on more evidence and reflects a higher degree of trust in *Y*, the distrust is also high, thus making the opinion about *Y* highly conflicting, and this may be one reason to reconsider the dependability of *T1*. Based on this discussion we can define degree of conflict about an opinion as:

$$\text{Conflict}\,(T) \;=\; 1 - \frac{|t-d|}{|t+d|} \qquad \text{where} \quad T \;=\; (t,\, d). \tag{10}$$

It is evident from this definition of conflict that the stronger the degree of support relative to the refutation degree the lesser is the conflict. For the same difference in the support and refutation degrees, the conflict increases with increase in evidence for trusting or distrusting the entity as is clear from the denominator. For example, considering two trust opinions $T1 = (0.5, 0.4)$ and $T2 = (0.3,0.2)$ though both lead to the conclusion about trustworthiness of the party with the same degree (**0.1**) for *T1* we are more confident of the conflict because it based on more proof and hence *T1* has a higher conflict than *T2*.

In the above discussion we identified two possible deterrents to dependable trust statements, namely ignorance (Policy 1) and conflict (Policy 2). The degree of refutation (Policy 3) might itself be viewed an indicator for unreliable trust judgments instead of conflict, since a higher refutation degree means more evidence opposing the popular belief about a user. Whereas conflict measures the difference between support and refutation, Policy 3 considers an opinion about the trustworthiness risky if the refutation is high irrespective of how high or low the support is. If a party is supposed to be trustworthy ($t > d$) then a higher distrust implies more risk. This differs from Policy 1 where for two trust opinions $T1 = (0.7,0.3)$ and $T2 = (0.2,0.1)$, *T2* would be regarded as more risky since the degree of conflict is higher, whereas with Policy 3, *T1* is the one which is less dependable, due to the higher degree of refutation irrespective of how high the support is. To formulate a rule for computing risk we investigate the effectiveness of various risk computation policies which may factor in the above three measures, in terms of providing dependable trust assessment and quality recommendations. We outline a few risk assessment policies below for trust statement $T = (t,\, d)$.

$$\left.\begin{array}{l} \text{Policy 1}: \text{Risk}(T) = \text{Conflict}(T) \\ \text{Policy 2}: \text{Risk}(T) = 1 - (t+d)\,(\text{Ignorance}) \\ \text{Policy 3}: \text{Risk}(T) = \min(t,d)\,(\text{Degree of Refutation}) \\ \text{Policy 4}: \text{Risk}(T) = \frac{\text{Ignorance}+\text{Conflict}}{2} \\ \text{Policy 5}: \text{Risk}(T) = \frac{\text{Ignorance}+\text{Degree of Refutation}}{2} \end{array}\right\} \tag{11}$$

The risk assessment policy 4 and 5 both consider a combination of ignorance with conflict and degree of refutation, respectively, by taking a simple average of the quantities.

4.2 Applying risk policy for reliable trust assessment

The risk policies discussed above try to quantify the amount of risk involved in depending on various trust statements as a function of ignorance, conflict and refutation degree. However, which policy works best may depend on the dataset and the context. Whichever policy is chosen to quantify the dependability of trust statements, the risk quantity can be utilized in the following two different ways:

1. When trying to judge the trustworthiness of a stranger, trust propagation is used to arrive at an opinion about the unknown person. While propagating trust, the

stranger could be reached via several trust paths. In such a case trust paths with lower risk can be chosen to get reliable indirect trust evaluation.

2. Prune the trust network to remove highly unreliable, risky statements so that all recommendations would be based on quality links.

We follow scheme (2) and utilize the risk assessment to remove risky edges. Scheme (1) would prove to be computationally more expensive since while computing trust between two users who are not directly connected, it would require all paths between the users to be enumerated and sorted to determine the "paths of low risk". The "high-risk" edges considered for elimination can either be chosen against a threshold, i.e., edges with risk below a threshold or we could choose the top $K\%$ of the "high risk" edges. However, the main limitation of the proposed approach is that inferring trust and distrust via trust propagation operates on the entire trust network. This means that it is necessary to compute the trust and distrust values for the full relationship graph of the users in the population in order to be able to compute indirect trust and distrust between distant users.

However, for data which is relatively static, such a trust network can be computed in an offline process and can be utilized to infer trust and distrust between users online. For dynamically changing ratings set, for estimating the trust and distrust degrees between a pair of distant users, say (A, B), a more appropriate technique would be to compute the quantities on the fly. Starting from A, evaluate each of its potential neighbors (those sharing common experiences with the user with respect to rating items or users or with whom A has a direct trust link) for the degree of trust and distrust that A has on them.

From among the neighbors, eliminate the top $K\%$ of risky links and utilize the rest to further propagate the trust and so on. Figure 3 presents the steps in the proposed trust–distrust based recommendation framework. The predicted rating (Step 4) is computed using Resnick's prediction formula (Resnick et al. 1994).

5 Experimental evaluation

In this section, we demonstrate the effectiveness of our trust computation techniques, for reaching out to a representative set of users that closely match the active user in his tastes and preferences. We establish the improvement in the recommendation quality through the proposed approach over those provided by the existing trust derivation mechanisms. Since our techniques utilize the preference as well as the trust and distrust information, we derive our data from the Extended Epinions dataset (http://www.trustlet.org/) collected by Paolo Massa.

5.1 Dataset

Epinions is a popular e-commerce website which allows users to read and write reviews on various products and services and also allows such reviewers to be rated by the other users. The article ratings scale is from 1 to 5. The dataset consists of 1,560,144 articles which are rated by 132,000 users who issued 13,668,319 article ratings. In addition, users can express their like or dislike of a reviewer by labeling him trust or distrust worthy and have issued 841,372 statements out of which 71,766 are trust and 123,705 are distrust statements. The ratings data, however, are skewed as most ratings in the dataset are 4 and 5.

More than three quarters of the ratings have a value of 5, whereas only 0.02% of the ratings are a 1. For such a skewed dataset a simple algorithm which predicts the item average every time might outperform the traditional collaborative filtering techniques (Massa and Avesani 2007). Hence, we randomly remove some of the majority ratings from the dataset to make it more balanced though retaining the bias towards rating values 4 and 5. From this modified dataset we select 1,000 users who have rated at least 10 movies and whose average rating is below 4. We endeavor to assess the effectiveness of proposed techniques in improving the accuracy of predictions as well as in their robustness against attacks. The following subsection presents an experimental comparison of prediction accuracy achieved by the proposed techniques against several baselines. Section 5.3 evaluates the effectiveness of the various approaches against different attacks on the RS.

5.2 Accuracy

The experiments were performed by splitting the user set into training users and active users. A portion of the active user's rating space is hidden and the system is asked to predict the ratings based on the voting data from the training users. The fraction of the active user's ratings to be predicted shall be varied to evaluate the system's performance across different configurations. To evaluate the prediction quality of the proposed system in comparison to the other prediction algorithms, we employ mean absolute error (MAE) and coverage. MAE measures the average absolute deviation of the predicted rating of an item from the actual rating and is defined as follows:

$$\text{MAE} = \frac{1}{|N|}\sum_{k=1}^{N}|pr_k - r_k| \tag{12}$$

where N is the number of hidden voting scores, pr_k is the predicted rating and r_k is the actual rating. A smaller value of MAE signifies better prediction quality. The total

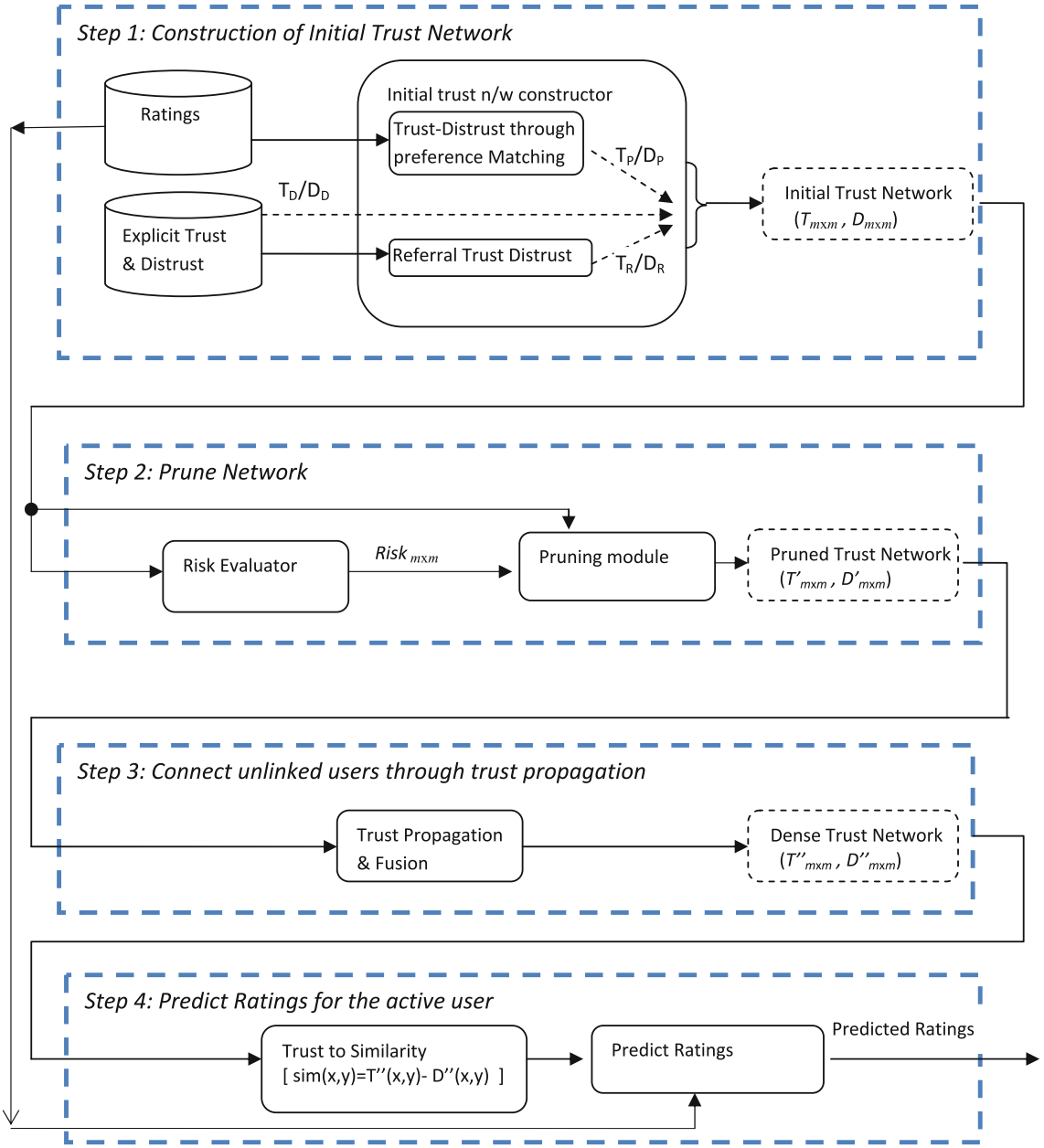

Fig. 3 Proposed trust–distrust based RS framework with 'm' users

coverage of the system is the percentage of predictions that a recommendation algorithm is able to achieve. High coverage corresponds to being able to predict opinions about more number of items and is defined as:

$$\text{Coverage} = \frac{p}{N}, \tag{13}$$

Here p is the number of predictions obtained, and N represents the number of unknown ratings to be predicted. For all experiments δ and ρ are set to 20. The number of neighbors considered in the k-nearest neighbor approach is set to 30. In all experiments a fraction of the active user's ratings, randomly chosen, are retained as training data and the rest are used for evaluating the various algorithms. Each experiment is run 10 times to rule out any run-specific bias.

5.2.1 Optimal parameter estimation

The trust network construction as proposed in our work incorporates the explicit trust statements, item preference data and the referral trust components and is modeled as a linear combination of trust derived from these three sources as shown in (3). The parameters α, β and γ represent the influence of the trust through preference, referral trust and

direct trust on the final trust and distrust values. In this experiment we plan to investigate the recommendation performance obtained while varying these parameters under varied data conditions and to find the optimum parameter values which minimize the prediction errors. To do so we vary the values of α, β and γ in increments of 0.2, so that each of α, β and γ take values in the set {0, 0.2, 0.4, 0.6, 0.8, 1} subject to constraint that $\alpha + \beta + \gamma = 1$. Thus, we get 21 such combinations. Note that combinations with a parameter 0 implies the corresponding component does not have any influence in the trust and distrust computation. In each configuration 50% of the users are active while the other 50% are used for training and for each active user half of his ratings are hidden and need to be predicted. Our experiments showed that among all combination of values (α, β, γ) = (0.2, 0.6, 0.2) results in the minimum MAE while being high on coverage as well. Hence, we choose this parameter setting for the rest of the experiments. It is to be noted that in the domain of recommender systems a small improvement in the predictive error can lead to significant improvement when ordering items by their predicted preferences (Koren 2008).

5.2.2 Comparison of local techniques

In this experiment we demonstrate the improvement in recommendations based on the ETN over predictions utilizing either trust and distrust scores or ratings. To compare the effectiveness of the proposed extension to the trust network, we compare it with surprisal-based vector similarity with significance weighting (SVSS) (Luo et al. 2008), the CF technique estimating the proximity in user tastes by employing their voting patterns. We also compare ETN with predictions obtained by using the explicitly specified trust relationships as a similarity estimate (Victor et al. 2009a). We henceforth term this method "Trust as Similarity" (TAS). The parameters α, β and γ for ETN are set to the values 0.2, 0.6 and 0.2, as determined in the previous experiment. As in the previous experiment half the users are active users while the other half are used for training. For SVSS the parameter γ was set to 20, as suggested by the authors. To analyze the comparative performance of the algorithms we show the resultant prediction error for varying levels of sparsity in ratings and trust scores. The sparsity levels in the ratings data are varied by retaining different portions of active user ratings set for neighborhood formation and predicting the rest. Hence, we retain 10, 20–90% of the ratings as scores already available to the system and the corresponding configurations are termed R10, R20–R90, respectively. Similarly, we vary sparsity in trust data by retaining 10, 20–100% of the trust statements and discarding the other trust and distrust links to obtain configurations T10, T20–T100.

The accuracy and coverage obtained by varying the sparsity in voting's data is shown in Figs. 4, 5 respectively. The accuracy results demonstrate the improvement using the proposed ETN method over the other two with varying sparsity levels. The performance of SVSS and TAS relative to each other, however, shows variation over the various configurations and there is no clear winner in terms of accuracy. It is to be noted that since TAS relies only on trust data for similarity estimation, its accuracy performance should not vary with change in ratings data, but Fig. 4 shows a decline in MAE with increase in rating density. However, this behavior can be attributed to the fact that we use the prediction formula as proposed by Resnick et al. (1994), which utilizes user ratings average data in the prediction process and hence a larger set of training ratings data would imply better estimation of user's average ratings. Figure 5 displays the coverage achieved by each of the techniques. The ability of ETN in connecting more user pairs is amply demonstrated by the coverage as shown in Fig. 5. ETN outperforms both TAS and SVSS in terms of coverage. We also note the decline in coverage of SVSS and ETN with increasing sparsity but as expected the coverage for TAS does not show any declining trend with variation in ratings sparsity.

The results of running the experiment while varying the sparsity in the trust data are displayed in Figs. 6 and 7. The ETN offers better prediction quality than both TAS and SVSS under most configurations. However, for T10 and T20 scenarios SVSS performs better. The lack of enough trust information in these two configurations would affect the explicit trust and referral trust components of the tri-component ETN and hence offers lower recommendation quality. The coverage of ETN is consistently superior to that of TAS and SVSS. The coverage percentage of ETN and TAS increases with decrease in sparsity but the coverage of SVSS remains steady.

5.2.3 Comparison of global techniques

In the previous experiment we analyzed the performance of techniques exploiting local user interrelationships in order

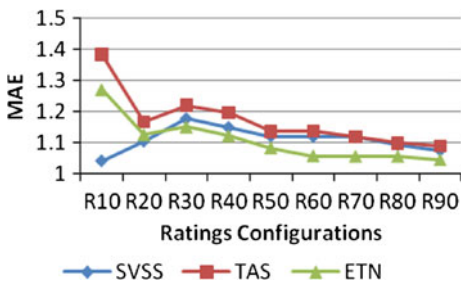

Fig. 4 Comparing MAE of SVSS, TAS and ETN under various ratings sparsity settings

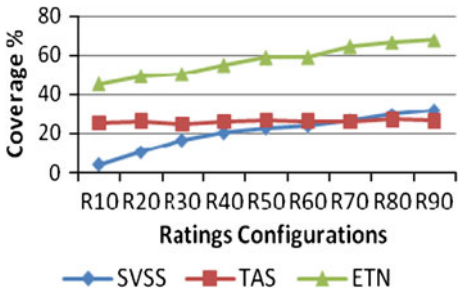

Fig. 5 Comparing coverage of SVSS, TAS and ETN under various ratings sparsity settings

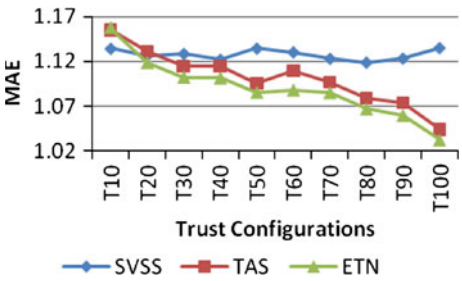

Fig. 6 Comparison of MAE for SVSS, TAS and ETN under various trust sparsity scenarios

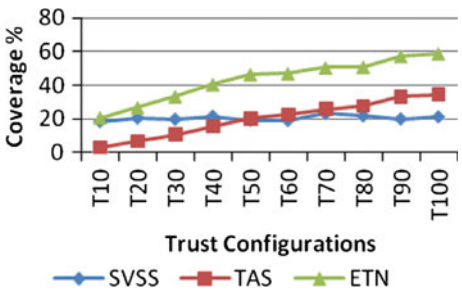

Fig. 7 Comparison of coverage for SVSS, TAS and ETN under various trust sparsity scenarios

to perform recommendations. The term "local" as utilized by (Luo et al. 2008) refers to techniques utilizing the immediately available voting patterns, trust elicitation, etc. to infer trustworthiness or like-mindedness between pairs of users. Global estimates of similarity (Luo et al. 2008) or trustworthiness on the other hand exploit the transitivity of trust and similarity to expand the user base participating in the recommendation process thus improving the quality and coverage of prediction. In the current experiment, we extend methods analyzed before by supplementing local user similarity computations with estimation of closeness exploiting the transitivity of similarity or trust and compare the performance of these global similarity estimation techniques. To demonstrate the improved performance achieved by TP-ETN, we compare it with the local–global similarity estimation technique (LS&GS) as proposed by Luo et al. (2008) and with MoleTrust Massa and Avesani (2007) as well as to recommendations obtained without trust propagation, i.e. ETN. The experimental setup is similar to the one in Sect. 5.2.2.

5.2.4 *Effectiveness of risk evaluation strategies*

The capability of the risk assessment schemes (Risk1–5) to eliminate low quality or weak connections between users is analyzed in this experiment. For LS&GS, the parameter α is set to 0.5 as suggested by the authors. The propagation horizon for MoleTrust and the TP-ETN is set to 2. The resultant MAE and coverage while varying sparsity in ratings and trust data is as shown in Figs. 8, 9, 10, 11.

As is evident from the figures, TP-ETN is able to achieve much higher accuracy while also maintaining a high coverage in most situations. Again it is evident that MAE for LS&GS shows no increasing or decreasing trend when the sparsity in trust is varied as LS&GS totally depends on ratings alone for similarity estimation.

Under very sparse ratings data scenario (R10), we note that both MoleTrust and LS&GS outperform TP-ETN, but their corresponding coverage is much lower. For highly dense data situations (R90), however, LS&GS is able to achieve higher coverage. Similarly, while varying the sparsity in trust data even though TP-ETN offers best accuracy consistently its coverage for the sparse trust data is lower than that of LS&GS (T10, T20).

The accuracy improvement they offer is weighed against their loss of coverage as opposed to propagation in a trust network without pruning. Hence the techniques Risk1–5 are compared against TP-ETN. For each of the algorithms using Risk1–5 the top 30% of the high-risk trust links are removed from the trust network, i.e. K is set to 30. Again, we compare the algorithms by varying the sparsity in the trust and ratings data and the experimental setting is similar to that of Sect. 5.2.3

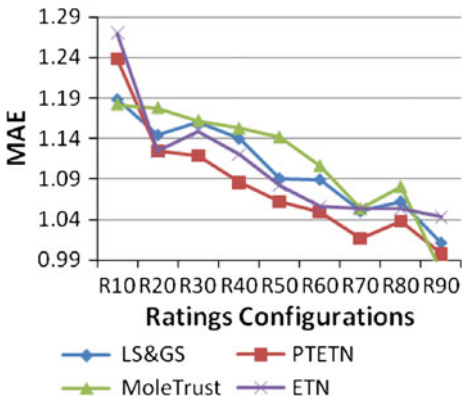

Fig. 8 Comparing MAE of LS&GS, TP-ETN, ETN MoleTrust and under various ratings sparsity settings

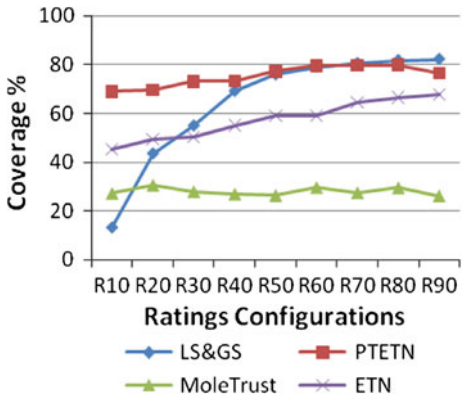

Fig. 9 Comparing coverage of LS&GS, TP-ETN, ETN MoleTrust and under various ratings sparsity settings

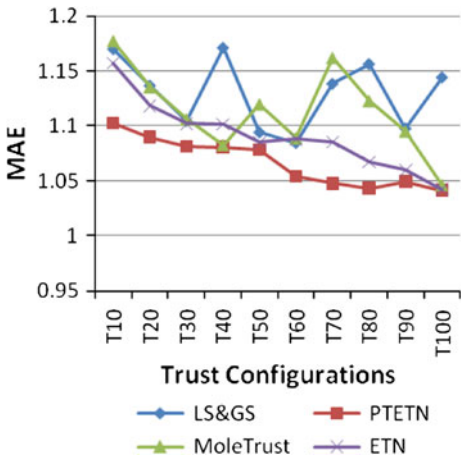

Fig. 10 Comparing MAE of LS&GS, TP-ETN, ETN MoleTrust and under various trust sparsity settings

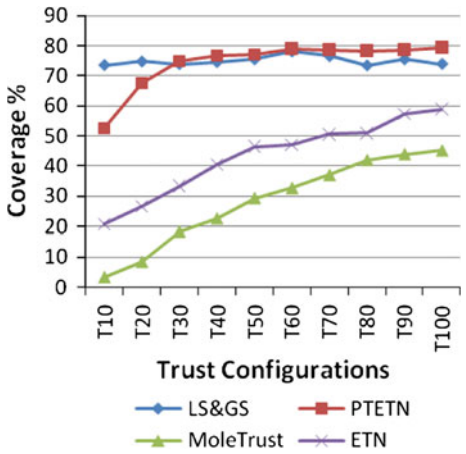

Fig. 11 Comparing coverage of LS&GS, TP-ETN, ETN MoleTrust and under various trust sparsity settings

The accuracy and coverage obtained by varying the rating sparseness is displayed in Table 1, whereas Table 2 shows the results achieved while varying the trust sparsity. It is to be noted that all tables highlight the best MAE and coverage scores obtained while comparing various algorithms in bold. Note that the least MAE is highlighted and similarly the highest coverage among the trust network pruning techniques is highlighted. TP-ETN always achieves the highest coverage since it always works on a denser trust network than the other schemes. The main idea here is to identify technique improving the accuracy while maintaining a comparable coverage.

A look at Table 2 shows under higher sparsity levels (R10–R60) Risk1 almost always achieves a better accuracy than TP-ETN, and the least MAE among all techniques, except for (R10 and R40). Thus, conflict is a good estimate of the reliability of trust statements when the ratings are sparse. Over denser ratings data settings (R80, R90) Risk5 is able to achieve higher accuracy. Among all pruning methods Risk1 almost always achieves the highest coverage. Under various sparsity conditions Risk1 seems to perform the best since it outperforms TP-ETN under most cases and also gives the highest coverage. However, a look at the overall performance under different sparsity conditions, obtained by averaging the MAE and coverage scores over all cases (R10–R90) (Table 3) reveals that Risk4 achieves the best accuracy overall. It achieves the highest improvement in accuracy over TP-ETN but suffers from a drop in coverage compared to Risk1. On observing Table 2, which shows comparison of the methods under varying trust sparseness again we note that the risk pruning techniques are effective in outperforming TP-ETN. Risk2 is able to give the best MAE under maximum number of cases, however, there is no clear trend indicating the pruning method to be adopted under various trust sparsity scenarios.

The overall performance scores (Table 4) over all trust sparsity environments, again show the best accuracy obtained by Risk4 strategy. The number of ratings predicted is the maximum for Risk1 as is indicated by its coverage and though it outperforms TP-ETN in some cases, the overall accuracy it offers, is worse than that of TP-ETN as shown in Table 4. It is to be noted that the sparseness in ratings data does not result in as much decrease in coverage as sparseness in trust data does. This may be due to the fact that trust data is used in two ways to assess the initial trust and distrust, i.e. functional and referral trust components and also because there are more trust links than ratings in the dataset. The overall performance of the strategies shown in Tables 3 and 4 highlights the best general performance of Risk4 strategy which is a combination of ignorance and conflict.

5.3 Robustness

In this section we aim to evaluate the proposed approaches with respect to their robustness against various kinds of

Table 1 Comparison of MAE and coverage of Risk1–5 and TP-ETN while varying ratings sparsity

Rating configurations	Risk1	Risk2	Risk3	Risk4	Risk5	TP-ETN
R10						
MAE	1.297361	1.232177	1.297408	**1.218061**	1.237655	1.328292
Coverage	65.9242	61.32	**67.7452**	62.1016	61.6454	0.689083
R20						
MAE	**1.119973**	1.157872	1.120986	1.150599	1.152308	1.124955
Coverage	**67.7575**	63.9707	65.3209	63.6077	63.365	69.6074
R30						
MAE	**1.109301**	1.144747	1.110234	1.130164	1.141443	1.118818
Coverage	**69.9802**	65.468	69.8323	65.3554	65.5512	73.0538
R40						
MAE	1.074986	1.07796	1.075992	**1.070938**	1.083226	1.085839
Coverage	**70.5473**	66.0028	69.8743	65.3469	65.5309	0.73357
R50						
MAE	**1.060929**	1.075573	1.070012	1.063892	1.079221	1.062506
Coverage	**75.1292**	69.5311	73.2439	67.1736	68.6641	0.77167
R60						
MAE	**1.046195**	1.074967	1.046231	1.080305	1.073963	1.049434
Coverage	**77.4114**	73.1086	76.5389	73.774	72.7656	79.4581
R70						
MAE	1.029663	1.045201	1.029987	**1.01353**	1.032823	1.016782
Coverage	**78.0144**	74.5575	77.8376	74.0611	73.6862	79.556
R80						
MAE	1.014214	1.011808	1.014312	1.011818	**1.008901**	1.03837
Coverage	**78.9765**	76.0149	75.4438	74.8816	75.7149	79.8432
R90						
MAE	0.996704	1.00989	0.991755	0.99945	**0.983649**	0.997755
Coverage	**74.92**	72.0233	73.1762	71.27	71.79	76.3867

attacks as discussed in Sect. 2.4. There have been several metrics which quantify the effectiveness of algorithms in reducing the impact of attacks (Mobasher et al. 2007). We use a metric named Prediction shift (PS) to evaluate the robustness of various algorithms. PS measures the change in the predicted ratings for a pushed (nuked) item induced by the attack profiles. If $p_{u,i}$ and $p'_{u,i}$, respectively, refer to the predicted rating of the item i by user u before and after the attack, respectively, then the prediction shift for user u for item i is defined as;

$$\text{PredShift}(u,i) = pr'_{u,i} - pr_{u,i} \tag{14}$$

A successful push attack would hence achieve a positive shift while a negative shift corresponds to a successful nuke attack. The prediction shift for item *i, PredShift(i),* is computed as the average of prediction shift over all active users for the item. The overall prediction shift for the system, *PredShift*, is then computed by averaging prediction shift for all targeted items.

The initial dataset for evaluating the robustness of various algorithms is derived as discussed in Sect. 5.1. For all attack models, the number of attack profiles is inserted in the ratings database according to the attack size which is the percent of the number of users in the system. The number of filler ratings is set to 6% of the total number of ratings. The number of selected items is set to 3% of the total number of items. The number of active users for all experiments is 50 and the number of attacked items is set to 50 as well.

To generate random attack profiles we set the ratings of 6% (filler) of the items to a random value between the maximum and minimum rating. The target movie is given the highest or lowest rating according to whether it is a push or a nuke attack. Average attack profiles are generated by choosing 6% of the movies and associating with each the average rating for the movie. Profiles for Bandwagon attacks are created by choosing the 20 most popular movies in the selected set where a movie is deemed popular which has the highest ratings and maximum numbers of users have rated it. The items in the selected set are associated with the highest ratings. The items in the filler set are

Table 2 Comparison of MAE and Coverage of Risk1–5 and TP-ETN while varying trust sparsity

Trust configurations	Risk1	Risk2	Risk3	Risk4	Risk5	TP-ETN
T10						
MAE	1.117598	**1.102573**	1.118965	1.112187	1.111332	1.102651
Coverage	**39.3358**	31.9543	37.3246	29.3749	30.6205	52.6571
T20						
MAE	1.092602	1.100514	1.10126	**1.049095**	1.096158	1.089724
Coverage	**54.4176**	46.7144	50.3267	45.6472	47.5009	67.6368
T30						
MAE	1.081251	**1.032396**	1.087251	1.034423	1.037562	1.081251
Coverage	**69.6887**	61.6747	69.537	59.2896	60.0973	74.8731
T40						
MAE	1.100469	**1.068246**	1.104387	1.074421	1.076305	1.080703
Coverage	**74.9222**	67.556	74.1284	67.1721	67.9427	76.6223
T50						
MAE	1.077721	1.085891	1.079865	**1.072739**	1.087283	1.078472
Coverage	**75.0573**	72.0217	73.9087	71.3736	71.7005	77.1039
T60						
MAE	**1.037358**	1.059833	1.040825	1.061133	1.057255	1.053687
Coverage	**76.9987**	73.9089	74.9008	73.1069	73.9409	79.0117
T70						
MAE	**1.039325**	1.048175	1.044264	1.041814	1.057039	1.047448
Coverage	**77.3664**	74.2573	75.363	74.5329	74.4554	78.699
T80						
MAE	1.042145	1.036539	1.042385	1.033275	**1.032079**	1.043236
Coverage	**77.5084**	75.8112	76.9088	75.792	75.7785	78.2817
T90						
MAE	1.073277	**1.023312**	1.065452	1.0523	1.030884	1.049244
Coverage	**77.45**	75.6764	77.1447	76.4536	76.2679	78.6824
T100						
MAE	1.051251	**1.002396**	1.052621	1.002744	1.006418	1.041251
Coverage	**78.358**	77.2651	77.6241	77.7739	77.6623	79.378

Table 3 Overall MAE and coverage comparison of Risk1–5 and TP-ETN under varying levels of sparsity in ratings data

	Risk1	Risk2	Risk3	Risk4	Risk5	TP-ETN
MAE	1.084258	1.092244	1.083808	**1.082084**	1.088132	1.091417
Coverage	**73.1845**	69.1108	72.1126	68.6191	68.7459	75.2597

Table 4 Overall MAE and coverage comparison of Risk1–5 and TP-ETN under varying levels of sparsity in trust

	Risk1	Risk2	Risk3	Risk4	Risk5	TP-ETN
MAE	1.0713	1.055988	1.073728	**1.053413**	1.059232	1.066767
Coverage	**70.11031**	65.684	68.71668	65.05167	65.59669	74.2946

conferred random ratings and the target items have the maximum rating. Reverse Bandwagon profiles are also created in a similar manner with low rating conferred upon the top 20 most disliked items. To choose the disliked items the 20 items with minimum average of ratings and which have been rated by at least 10 people, are chosen.

In the following experiments we compare the performance of SVSS, ETN, LS&GS, Risk1–5, and TP-ETN.

We do not include TAS and MoleTrust in the comparison because we assume that the attack profiles are unable able to garner trust and distrust statements from any genuine user. Under such an assumption the predictions achieved by TAS and MoleTrust are totally uninfluenced by the attack profiles since their similarity computation is independent of the ratings data.

5.3.1 *Effect of attack size*

Even though creating an unlimited number of attack profiles in a system is pretty hard, a reasonable attack size can hugely influence the ratings for the attacked item and subsequently affect the trustworthiness of the RS. In this subsection we investigate the effect of the attack size (the number of attack profiles) on the prediction shift for various algorithms. To do this we consider attack sizes 5, 10, 15, 20, 25 and 30% of the number of users in the system. The parameters (α, β, γ) are set to the optimal value of (0.2, 0.6, 0.2) as determined in experiment 5.2.1. We evaluate the effect the attack sizes in case of random, average, bandwagon and reverse bandwagon attacks.

Figures 12, 13, 14, 15 show the effect of random, average, bandwagon and reverse bandwagon attacks, respectively, for various attack sizes. In all cases, as expected, the shift in predictions increases with the increase in the size of attacks. Also in all cases, strategies employing only preference matching (SVSS & LS&GS) perform much worser than the proposed approaches which employ ratings, trust and distrust information. We note that among all push attack strategies average prediction achieves the maximum shift in general. This is since average attack is based on more knowledge about item averages and hence is more successful. In all cases we can also see the local approaches perform better than global approaches, e.g. SVSS achieves lesser prediction

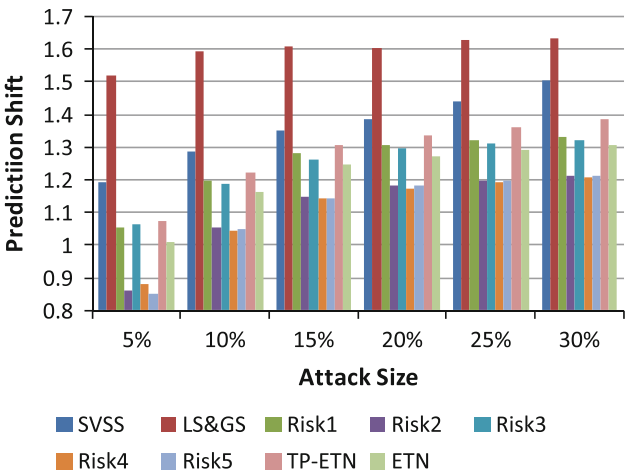

Fig. 12 Comparison of PS of SVSS, LS &GS, Risk1–5, TP-ETN & ETN under average attack for varying attack sizes

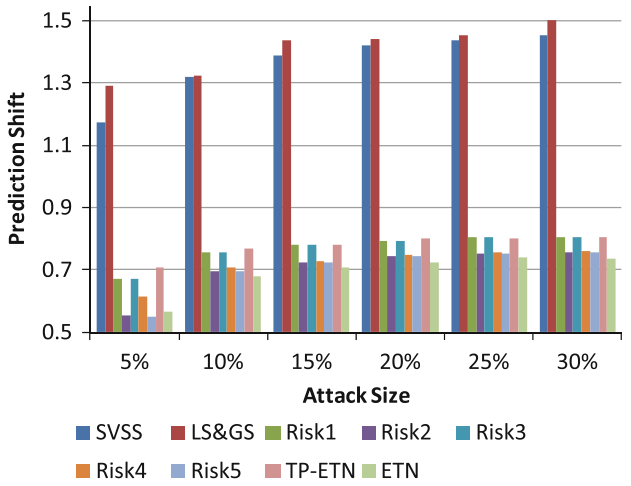

Fig. 13 Comparison of PS of SVSS, LS &GS, Risk1–5, TP-ETN & ETN under random attack for varying attack sizes

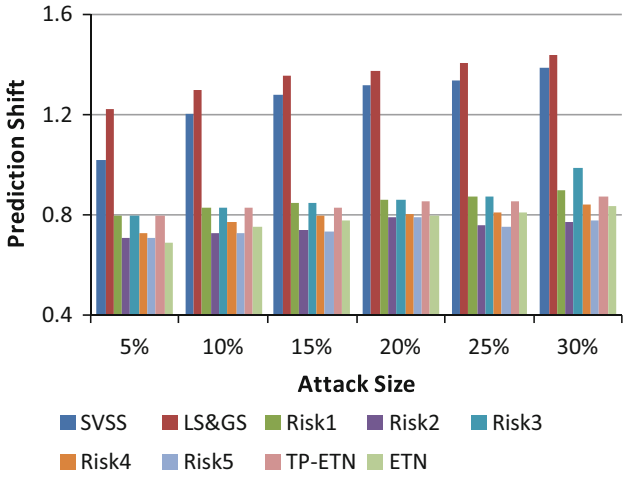

Fig. 14 Comparison of PS of SVSS, LS &GS, Risk1–5, TP-ETN & ETN under average attack for varying attack sizes

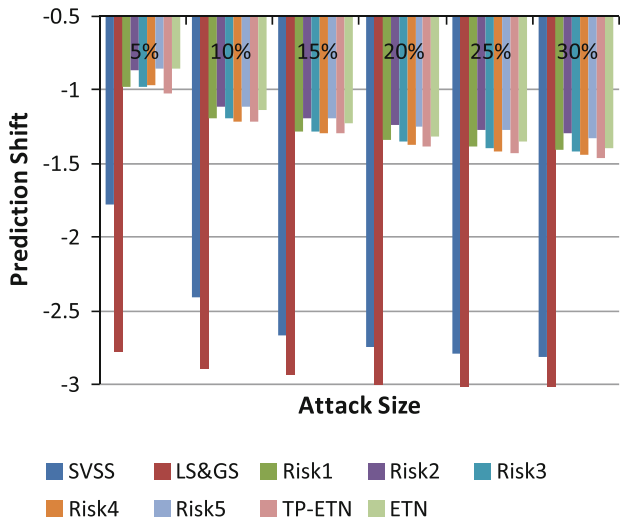

Fig. 15 Comparison of PS of SVSS, LS &GS, Risk1–5, TP-ETN & ETN under random attack for varying attack sizes

shift than the corresponding LS&GS and the prediction shift for ETN is lesser than that for TP-ETN. This may be because global approaches may lead to an increase in connection strength between any pair of users by exploiting different paths connecting them and thus might lead to higher similarity between a genuine and an attack profile. However, we observe that introduction of pruning criteria for TP-ETN decreases the prediction shift. Especially the policies employing ignorance in the risk computation (Risk2, Risk4 and Risk5) perform best for all types of attacks.

This can be explained as follows. When computing the measure of trust and distrust between a genuine and an attack profile the only factor contributing to trust and distrust is the T_P and D_P (trust through preference matching), respectively. Since T_D, D_D, T_R and D_R are all 0 (we assume that there are no trust links from actual users to fake user profiles), the actual trust and distrust values will be small (Eq. 4). This means that for the derived ETN values from all users to the fake users the ignorance is very high and hence Risk2, 4 and 5 evaluate to high values. This ensures that most connections to the fake user profiles are severed. In fact Risk2, 4 and 5 are able to achieve slightly lower prediction shift than the ETN (local similarity) for all attack types except for random attacks when ETN achieves the lowest shift.

The relative advantage offered by Risk2, 4 and 5 compared to the other global strategies is maximum under smaller attack sizes, and decreases with increased attack size.

5.3.2 *Effect of parameter α*

The parameter α adjusts the influence of the trust and distrust components derived from ratings in the final trust and distrust computation. In this subsection we examine the effects of increasing α on the effectiveness of the various types of attacks. We perform this experiment by varying

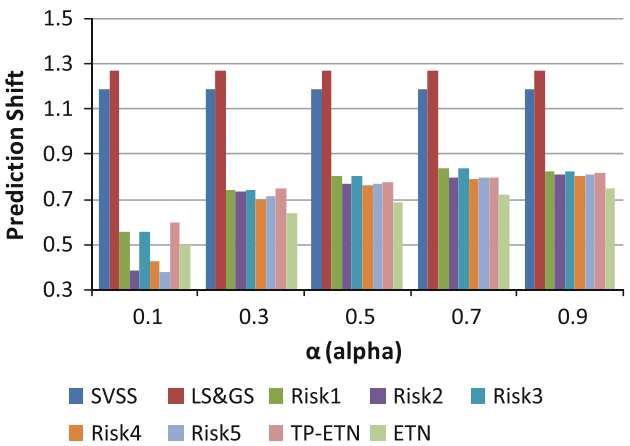

Fig. 16 Comparison of PS of SVSS, LS &GS, Risk1–5, TP-ETN & ETN under average attack for varying α

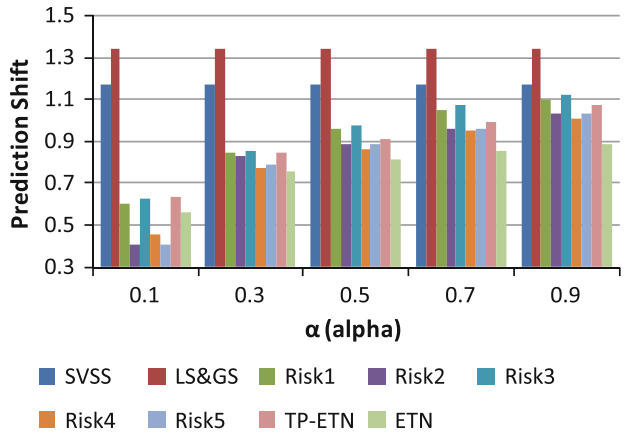

Fig. 17 Comparison of PS of SVSS, LS &GS, Risk1–5, TP-ETN & ETN under random attack for varying α

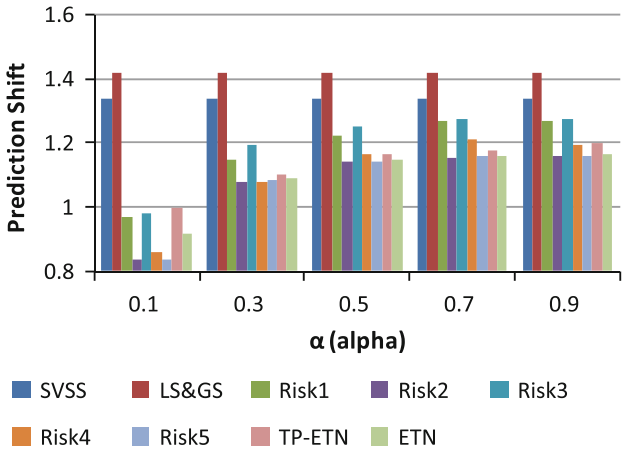

Fig. 18 Comparison of PS of SVSS, LS &GS, Risk1–5, TP-ETN & ETN under bandwagon attack for varying α

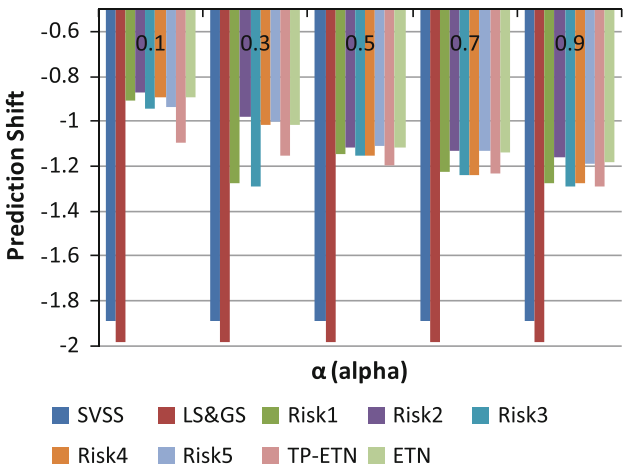

Fig. 19 Comparison of PS of SVSS, LS &GS, Risk1–5, TP-ETN & ETN under reverse bandwagon attack for varying α

the value of α in the set {0.1, 0.3, 0.5, 0.7 and 0.9}. The other parameters β and γ are computed as $\beta = \gamma = (1 - \alpha)/2$, the attack size if set to 5% and the rest of the parameters are fixed as described in Sect. 5.3.1. Figures 16, 17, 18, 19 plot the prediction shift with varying values of α for average, random, bandwagon and reverse bandwagon attacks, respectively. In all cases, it can be observed that with increasing α the prediction shift also increases. This is because an increase in the value of α would increase the influence of ratings in determining user tie strength and consequently would lower the influence of links derived from directly expressed trust–distrust information (β and γ).

6 Conclusion

In this work, we detailed an approach utilizing user-expressed opinions about other entities to overcome the sparsity-inherent challenges which exist in web-based systems. Our contribution is twofold. Firstly, we propose a system to deduce trusting or distrusting relationships among users from voting patterns as well as user-expressed trust judgments. The proposed tri-component trust and distrust estimation technique not only achieves improvement in the quality of recommendations but is also able to infer more trust bonds between unconnected users. Secondly, from the trust bonds inferred between users by utilizing extended trust network (ETN), we propose to sever low-quality links between users by quantifying the risk in heeding to the trust judgments inferred. We put forth several risk evaluation schemes which are modeled as a function of ignorance, conflict and degree of refutation in the opinions about an entity. Under TP-ETN the removal of such high-risk edges results in more reliable trust judgments inferred through trust propagation. Evaluation of the proposed framework against several baselines demonstrate that our system is able to establish more effective links among users and thus provide better recommendations.

As future work, we would like to explore the various alternative ways, as discussed in Sect. 4.2, in which reliability of the issued trust statements can be used to fine-tune the trust and distrust degrees among users. An interesting future direction would be to automatically estimate the parameters α, β and γ for the optimal combination of the three components contributing to the trust computation based on the data density and context. Learning techniques such as GA could be applied to learn such optimal set of parameters(Anand and Bharadwaj 2011). The possibility of combining the advantages offered by each of the risk assessment policies by analyzing more deeply into which situations each would best work in can also be explored. It would also be interesting to experiment with other trust inference schemes to further improve the performance of the system. Another direction could be to expand the set of information sources on the basis of which user relationships can be determined, such as content information or tag data, etc.

References

Adomavicius G, Tuzhilin A (2005) Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions. IEEE Trans Knowl Data Eng 17(6):734–749

Al-Shamri MYH, Bharadwaj KK (2008) Fuzzy-Genetic Approach to Recommender System Based on a Novel Hybrid User Model. Expert Systems with Applications, Elsevier 35(3):1386–1399

Anand D, Bharadwaj KK (2010a) Enhancing accuracy of recommender system through adaptive similarity measures based on hybrid features, In: Proceedings of 2nd Asian conference on intelligent information and database systems (ACIIDS 2010). LNAI 5991:1–10

Anand D, Bharadwaj KK (2010b) Adaptive user similarity measures for recommender systems: a genetic programming approach. In: Proceedings 3rd IEEE international conference on Computer Science and Information Technology, pp 121–125, IEEE

Anand D, Bharadwaj KK (2011) Utilizing various sparsity measures for enhancing accuracy of collaborative recommender systems based on local and global similarities. Expert Syst Appl 38:5101–5109

Bell RM, Koren Y, Volinsky C (2007) Modeling relationships at multiple scales to improve accuracy of large recommender systems. In: Proc. 13th ACM SIGKDD international conference on knowledge discovery and data mining, ACM, pp 95–108

Bharadwaj KK, Al-Shamri MYH (2009) Fuzzy computational models for trust and reputation systems. Electron Commer Res Appl 8(1):37–47

Breese JS, Heckerman D, Kadie C (1998) Empirical analysis of predictive algorithms for collaborative filtering. In: Proceedings of 14th annual conference on uncertainty in artificial intelligence, Morgan Kaufmann, San Fransisco, pp 43–52

Burke R (2002) Hybrid recommender systems: survey and experiments. User Model User-Adapt Interact 12(4):331–370

Cantador I, Bellogín A, Vallet D (2010) Content-based recommendation in social tagging systems. In: Proceedings of the fourth ACM conference on recommender systems, Barcelona, ACM, pp 237–240

Chen L, Qi L (2011) Social opinion mining for supporting buyers' complex decision making: exploratory user study and algorithm comparison. Soc Netw Anal Min 1:301–320. doi:10.1007/s13278-011-0023-y

Dell'Amico M, Capra L (2008) SOFIA: social filtering for robust recommendations. In: Proceedings of international federation of information processing (IFIP), Trust Management II, Springer, pp 135–150. doi:10.1007/978-0-387-09428-1_9

Esslimani I, Brun A, Boyer A (2010) Densifying a behavioral recommender system by social networks link prediction methods. Soc Netw Anal Min, Springer, 1(3):159–172. doi:10.1007/s13278-010-0004-6

Gambetta D (2000) Can we trust trust?, Gambetta D (ed) Trust: making and breaking cooperative relations, Department of Sociology, University of Oxford, chapter 13, pp 213–237

Golbeck J (2005) Computing and applying trust in web-based social networks. PhD thesis

Golbeck J, Parsia B, Hendler J (2003) Trust networks on the semantic web. In: Proceedings of cooperative intelligent agents, Helsinki, Finland, LNAI 2782, pp 238–249

Gray E, Seigneur J, Chen Y, Jensen C (2003) Trust propagation in small worlds. In: Proceedings of the first international conference in trust management, LNCS, vol 2692, pp 239–254, Springer

Guha R, Kumar R, Raghavan P, Tomkins A (2004) Propagation of trust and distrust. In: Proceedings of the 13th International World Wide Web Conference, ACM, pp 403–412

Gutscher A (2009) Reasoning with uncertain and conflicting opinions in open reputation systems. Electron Notes Theor Comput Sci 244:67–79

Hamouda S, Wanas N (2011) PUT-Tag: personalized user-centric tag recommendation for social bookmarking systems. Soc Netw Anal Min, Springer, 1(4):377–385. doi:10.1007/s13278-011-0028-6

Jamali M, Ester M (2009) Using a trust network to improve top-N recommendation. In: Proceedings of the third ACM conference on recommender systems, ACM, pp 181–188

Jøsang A, Lo Presti S (2004) Analyzing the relationship between risk and trust. In: Proceedings of the 2nd international conference on trust management, pp 135–145

Jøsang A, Hayward R, Pope S (2006a) Exploring different types of trust propagation, trust management, LNCS 3986, Springer, pp 179–192

Jøsang A, Hayward R, Pope S (2006b) Trust network analysis with subjective logic. In: Proceedings of the 29th Australasian computer science conference, Australian Computer Society Inc., pp 85–94

Jøsang A, Diaz J, Rifqi M (2010) Cumulative and averaging fusion of beliefs. Inf Fusion 11(2):192–200

Kayaalp M, Özyer T, Özyer ST (2011) A mash-up application utilizing hybridized filtering techniques for recommending events at a social networking site. Soc Netw Anal Min 1(3):231–239

Konstas I, Stathopoulos V, Jose JM (2009) On social networks and collaborative recommendation, In: Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval, Boston, ACM, pp 195–202

Koren Y (2008) Tutorial on recent progress in collaborative filtering. In: Proceedings of the 2008 ACM conference on recommender systems (ACM Recsys'08), pp 333–334

Lin Z, Ruchuan W, Haiyan W, Ruchuan W (2008) Trusted decision mechanism based on fuzzy logic for open network. J Comput 3(12):76–83

Liu B, Yuan Z (2010) Incorporating social networks and user opinions for collaborative recommendation: local trust network based method In: Proceedings of the workshop on context-aware movie recommendation, Barcelona, Spain, ACM, pp 53–56

Luo H, Niu C, Shen R, Ullrich C (2008) A collaborative filtering framework based on both local user similarity and global user similarity. Mach Learn 72(3):231–245

Massa P, Avesani P (2007) Trust-aware recommender systems. In: Proceedings of the 2007 ACM conference on Recommender system, ACM, pp 17–24

Matsuo Y, Yamamoto H (2009) Community gravity: measuring bidirectional effects by trust and rating on online social networks. In: Proceedings of the 18th international conference on World wide web, Madrid, Spain, ACM, pp 751–760

Matt P, Morge M, Toni F (2010) Combining statistics and arguments to compute trust, In: Proceedings of 9th International Conference on autonomous agents and multiagent systems (AAMAS 2010), Toronto, Canada, pp 209–216

Metaxas P (2009) Using propagation of distrust to find untrustworthy web neighborhoods. In: Proceedings of the 2009 fourth international conference on internet and web applications and services, IEEE Computer Society, USA, pp 516–521

Mobasher B, Burke R, Bhaumik R, Sandvig J (2007) Attacks and remedies in collaborative recommendation. IEEE Intell Syst 22(3):56–63

Pitsilis G, Knapskog SJ (2009) Social trust as a solution to address sparsity-inherent problems of recommender systems. ACM RecSys 2009 Workshop on Recommender Systems and The Social Web, ACM

Prade H (2007) A qualitative bipolar argumentative view of trust, scalable uncertainity management, LNAI 4772, Springer, pp 268–276

Qiu X, Zhang L, Wang S, Qian G (2010) A Trust Transitivity Model Based-on Dempster-Shafer Theory, Journal of Networks, Vol 5(9), 1025–1032

Resnick P, Iakovou N, Sushak M, Bergstrom P, and Riedl J (1994) GroupLens: an open architecture for collaborative filtering of netnews. In: Proceedings of 1994 computer supported cooperative work conference

Shafer G (1976) A mathematical theory of evidence. Princeton Univ Press, Princeton

Symeonidis P, Tiakas E, Manolopoulos Y (2010) Transitive node similarity for link prediction in social networks with positive and negative links. In: Proceedings of the fourth ACM conference on recommender systems, ACM, pp 183–190

Victor P (2010) Trust networks for recommender systems. PhD thesis

Victor P, Cornelis C, De Cock M, Teredesai AM (2009a) Trust and Distrust based recommendations for controversial reviews. In: Proceedings of the Web Science Conference

Victor P, Cornelis C, De Cock M, Da Silva P (2009b) Gradual trust and distrust in recommender systems. Fuzzy Sets Syst 160:1367–1382

Wang Y, Singh MP (2010) Evidence-based trust: a mathematical model geared for multiagent systems. ACM Transactions on Autonomous and Adaptive Systems, 5(4)

Wang J, Sun H (2009) A new evidential trust model for open communities. Comput Stand Interf 31:994–1001

Wu B, Goel V, Davison BD (2006) Propagating trust and distrust to demote web spam. In: Proceedings models of trust for the web workshop (MTW), International World Wide Web Conference

Yu B, Singh MP (2002) Distributed reputation management for electronic commerce. Comput Intell 18(4):535–549

Yu B, Kallurkar S, Flo R (2008) A Dempster–Shafer approach to provenance-aware trust assessment. In: International symposium on collaborative technologies and systems, Inst. of Elec. and Elec. Eng. Computer Society, Irvine, CA, pp 383–390

Zhao S, Zhou MX, Yuan Q, Zhang X, Zheng W, Fu R (2010) Who is talking about what: social map-based recommendation for content-centric social websites. In: Proceedings of the fourth ACM conference on recommender systems, Barcelona, ACM, pp 143–150