Assessing the Credibility of Nodes on Multiple-Relational Social Networks

Weishu Hu and Zhiguo Gong

Department of Computer and Information Science, University of Macau,
Av. Padre Tomás Pereira Taipa, Macau
{yb07405,fstzgg}@umac.mo
http://www.fst.umac.mo/cis

Abstract. With the development of the Internet, social network is changing people's daily lives. In many social networks, the relationships between nodes can be measured. It is an important application to predict trust link, find the most reliable node and rank nodes. In order to implement those applications, it is crucial to assess the credibility of a node. The credibility of a node is denoted as the expected value, which can be evaluated by similarities between the node and its neighbors. That means the credibility of a node is high while its behaviors are reasonable. When multiple-relational networks are becoming prevalent, we observe that it is possible to apply more relations to improve the performance of assessing the credibility of nodes. We found that trust values among one type of nodes and similarity scores among different types of nodes reinforce each other towards better and more meaningful results. In this paper, we introduce a framework that computes the credibility of nodes on a multiple-relational network. The experiment result on real data shows that our framework is effective.

Keywords: Trust-based network, credibility, similarity, social network.

1 Introduction

People are used to sharing all kinds of content such as message, images, songs, video, opinions and blogs on different social networks e.g. Facebook, Twitter and YouTube. In these social networks, the reputation of a publisher plays an important role; otherwise, a user may receive some disgusting content such as virus and Trojan horse. Thus, the trust of a node granted by other users is a vital property of it. For example, there are explicit opinions on other users as trust/distrust on Slashdot and Epinions networks.

Unfortunately, online content is not always trustable. And it is no way to ensure the validity of the information on the Internet. Even worse, different users usually provide conflicting opinions, as following two examples.

Example 1 (Battery of IPhone). Suppose a user plans to buy an IPhone and reads the product review from Epionions.com. Among the top 20 opinions, he or she will find the following comments: three users say "Battery life suffers under

B. Benatallah et al. (Eds.): WISE 2014, Part II, LNCS 8787, pp. 62–77, 2014.

heavy use", four users say "Pretty long battery life", one says "The battery life on the phone drains really easily", and another one says "Increased battery life". Which suggestion should the user adopt?

Example 2 (Definition of Spam). We want to know what is spam? We notice that various definitions from different websites, so we show some of them in Table 1. From the integrity of expression, we found that typepad.com provides the most precise information. In comparison, the information from ask.com is incomplete, and that from Wikipedia is incorrect.

Table 1. Conflicting information about Spam

Web Site	Definition of Spam
Wikipedia	Spam is a canned precooked meat product made by the Hormel Foods Corporation, first introduced in 1937.
about.com	Spam is the practice of purposely deceiving a search engine into returning a result that is unrelated to a users query, or that is ranked artificially high in the result set.
ask.com	Spamming is a fairly easy task which involves a mass sending of a message, for any number of purposes.
webopedia.com	Spam is electronic junk mail or junk newsgroup postings.
typepad.com	Spam is commercial, unsolicited, unanticipated, irrelevant messaging, sent in bulk.

The Credibility Problem of the Internet has been acquainted by current network users. Princeton Survey Research [1] made a survey on the credibility of websites. The conclusion shows no less than 54% online users' trust news sites in most of the time, comparing to only 26% for sales websites and is barely 12% for blogs.

According to authority (or popularity) based on hyperlinks, there are many researches on ranking web pages. The most famous techniques are HITS [2], and PageRank [3] applied in Google.com. These two studies provide high scores to nodes having better connectivity. But unfortunately, authority does not lead to credibility of information. High ranked websites are usually the most popular ones. However, popularity does not equal to credibility. In trust-based networks, a highly nasty node may also have good connectivity but have a low credibility. It means that the credibility of one node depends on the opinions of other nodes, and also depends on how the node makes a fair evaluation about other nodes. In fact, a node with higher credibility should be as trustworthy as another similar node.

Belief propagation (sum-product message passing) is a message passing algorithm, which is used for performing inference on graphical models including Bayesian networks and Markov random fields. It computes the marginal distribution for each unobserved node based on other observed nodes. In addition, beliefs are the estimated marginal probabilities. Belief propagation is mainly

applied in information theory and artificial intelligence, which is demonstrated empirical success in numerous applications such as free energy approximation, low-density parity-check codes, turbo codes and satisfaction [4]. Belief propagation is not suitable for creditability problem, because of a lack of observed nodes in advance.

The trust-based network is very different from common network, and it is actually a directed graph. Trust-based network is a special social network having explicit links to express one node trusts/distrusts other nodes. The nodes are individual users, with the relationship "User X trusts User Y" resulting in an edge directed from User X's node to User Y's. Everything happens in some reasons, there is no absolutely independent behavior without any cause. We believe that one user trusts others for some sake, and we can observe that they have similar opinions, common friends or like the same items on these social networks. In a network such as Facebook and Twitter, an explicit link implies that two nodes are close for their frequent communication. However, in a trust-based network, two nodes may be closely connected but the link may show unreasonable. More importantly, a reasonable trust link in trust-based network is the two connected nodes have similar opinions or behaviors (make friends with the same users, focus on the same items). If two users are similar in terms of their opinions or other behaviors, then their trust links are more reasonable. In the other way, users have similar opinions or behaviors, and they don't have to trust each other. For instance, user A, B, C and D have trust relations as Fig. 1. It is intuitive that the trust link from A to B is more reasonable than that from C to D. Because D has no similar behaviors as C (C has two inlinks while D has nothing), the trust link from C to D is not reasonable. A and B have similar behaviors (they are trusting and trusted by the same user C).

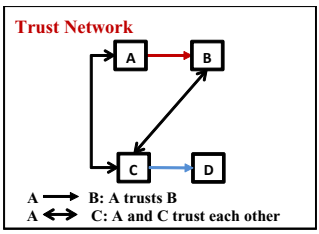


Fig. 1. An Example of Trust-Based Network

Trust is a measure of confidence that an entity or entities will behave in an expected manner [5]. Trust has emerged as a major impediment to the success of electronic markets and communities where interaction with the strangers is the norm [6]. Recently, a novel algorithm known as TrustRank is proposed for combatting web spam. However, the weakness of TrustRank is sensitive to the seed set, which could not be completely involved the different topics on the Internet. Moreover, TrustRank prefers to larger communities with prejudice for a given seed set.

In a rating system such as IMDB, Slashdot and Epinions, users can rate objects. A movie is an object in IMDB, and a product could be an object in Epinions and Slashdot. In other situations, each user can comment on other users and get feedbacks from them. The credibility of a user is depended on the feedbacks from other users, which can be considered as the inlinks of a user received. The attitude of a user about others is based on his comments (outlinks). In an isolate consideration, credibility of a user depends on the quality of inlinks and fairness of a user who has made an opinion towards him, no matter the quantity. In other words, the fairness depends on the opinion he gives in the form of outlinks. If a user is unfair, then his opinion should weigh less. Then, the credibility of another user mainly relies on the links from truthful users. A user that only gives groundless opinions irrespective of the similarities between other users and him is highly injustice. Similarly, a user receiving groundless inlinks from highly unfair users has a lower credibility than a user receiving inlinks from reliable users. In some extreme cases, a user may receive all high credibility but still express his opinion on another user that differs from all other users' in the network.

When the multiple-relational network is coming up all over the world, we observe that it is not only requisite but also advantageous to combine the trust and similarity analysis into one framework because we can apply information from one side to improve the other side. In our case, due to the multiple-relation nature of the network, when computing the similarity of one type of nodes, we should put the trust of the other type of nodes into the formulation. This leads to an asymmetric similarity formulation. This approach has never been studied before. As we analyzed in the above subsection, introducing similarity to trust analysis in a multiple-relational network could be beneficial to many key aspects on the trust analysis. Furthermore, similarity measure gets more customized information from trust analysis side, which should potentially be beneficial too. Our experiment results confirm this mutual beneficial relation.

Similarity and Trust computation can benefit each other, which motivates us to study how to effectively combine them together in one framework. Our technique adopts reinforcement scheme on the top of multiple-relational network decomposing. To be more detail, we firstly define a special bi-typed multiple-relational network as Trust Similarity (TS) network; then we decompose its different types of nodes into two homogeneous networks based on their relations, and we do the analysis of social trust spreading on the Trust network and expectation of similarity measures on the Similarity network. However, the two networks are not totally separated. There is a latent tunnel connecting them for the sake of delivering information back and forth to improve the performance trust and similarity analysis.

In Fig. 2, Alice and Bob trust each other, while Bob trusts Tom and Alice trusts Tom. Alice rates two products (IPad, Bag) and comments on one of Tom's reviews; Bob rates two products (Telephone, IPad) and comments on one of Alice's reviews; and Tom rates three products (Telephone, IPad, and Bag). There are three relations (Trust, Rating, and Comment) in Epinions Network. A reasonable trust between users should base on their similar behaviors. For example,

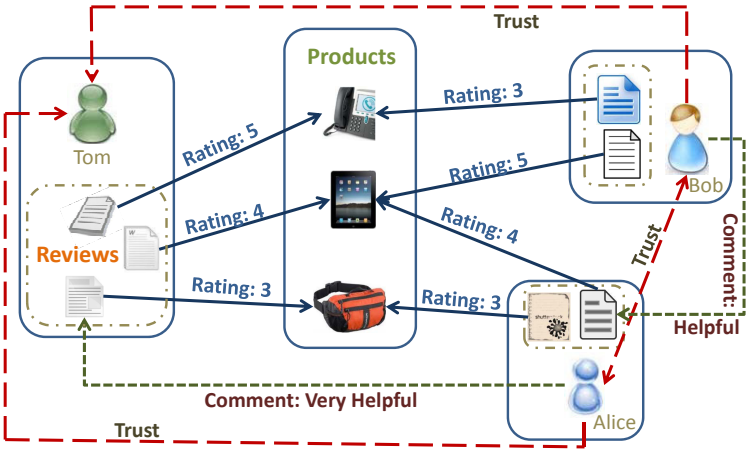


Fig. 2. An Illustration of Multiple-Relational Network of Epinions

they are trusted by the same users, give similar rating to the same products, or make similar comment on the same review. In this example, Alice trusts Tom is more reasonable than Bob trusts Tom, because Alice and Tom rate the same products with the same scores, and Alice makes a comment (very helpful) on Tom's rating, while Bob's rating is very different from Tom's.

We summarize our major contributions as follows.

- We present a model that computes the credibility of nodes in a multiple-relational network. The basic idea is the opinions of trustworthy nodes weigh more. The trustworthiness of a node is computed by the credibility of its neighbors. We observe that the credibility of a node depends on its behaviors, and a reasonable behavior is based on the similarity.
- We propose a new viewpoint of treating trust and similarity computation together. To our best knowledge, our work is leading to explicitly explore how to make use of both two techniques together to analyze a multiple-relational network in a more comprehensive way.
- We study the mutual improvements of trust analysis and similarity computation on each other. An iterative algorithm with optimization on decomposed multiple-relational networks is suitable for this reinforcement relationship.
- We demonstrate its effectiveness through real world social network analysis. Our method outperforms state of the art in trust analysis and similarity computation when they are performed separately.

The paper is organized as follows. We present the related works in Section 2. Section 3 describes the algorithm. Section 4 presents the experimental results before Section 5 concludes.

2 Related Works

Graph theoretic methods for ranking nodes in a network have gained popularity since the application of HITS [2] and PageRank [3] algorithms. As a result, a number of other methods have also been proposed. Most of these methods are usually a variant of eigenvector centrality measure [7]. The algorithm EigenTrust [8, 9] removes negative entries by not considering negative ratings. Ranking has been done on trust-based network as well while considering negative links, e.g. PageTrust [10]. The authors of [11] propose an algorithm to compute trust/distrust between two objects. There have been some studies on the social aspects of trust-based networks. One important example is the balance theory [12] that considers relationships of type "enemy of an enemy" as a friend. Another popular theory is status theory [13], where a positive link denotes higher status. These theories have been well evaluated in [14, 15]. [16, 17] compute the bias and prestige of nodes in simple networks where the edge weight denotes the trust score. These methods emphasize on single relation and neglect comprehensive utilization of multiple relations.

For anomaly detection and classification in numerous settings such as calling-card fraud, accounting fraud and cyber-security, guilt-by-association methods [18] derive stronger signal from weak ones. The authors focus on comparing and assessing three very effective algorithms: Random Walk with Restarts, Semi-Supervised Learning and Belief Propagation (BP). Their main contributions are two aspects: firstly, they theoretically prove that the three algorithms are effective in a similar matrix inversion problem; secondly, in practice, they propose a fast convergence algorithm called FaBP, which runs twice as efficient with equal or higher accuracy than BP. They show the advantage in synthetic and real datasets (YahooWeb). Guilt-by-association methods do not apply to Credibility Problem. The premise of guilt-by-association is like attracts like, but unreliable users try their best to get close to reliable ones in trust network, which leads to unreliable users may obtain high credibility. Besides, most of guilt-by-association methods needs supervised or semi-supervised.

TrustRank introduced in [19] is used for web spam, which is also related to Credibility Problem. Web spam is cheating behavior that finds ways to acquire top ranking by using loopholes of search engine ranking algorithms. The basic idea of TrustRank is that good websites seldom point to spam websites and people believe in these good websites. This confidence can be spread through the link topology on the network. Hence, a set of websites with high trustworthiness are picked to make up the seed set and each of them is initialized a non-zero trust value, while all the other websites on the network are assigned an initial value 0. Then a biased PageRank algorithm is used to propagate the initial trust values to their outgoing websites. When convergence, good websites will obtain higher trust values, and spam websites are tend to obtain lower trust values. The results show that TrustRank improves upon PageRank by maintaining good sites in top buckets, while most spam websites are moved to lower buckets. In an enhanced TrustRank [20], the authors propose Topical TrustRank, which applies topical information to partition the seed set and compute trust scores for each different

topic respectively. The combination of these trust scores for a website or page is used to decide its ranking. Their experimental results on two large datasets indicate that Topical TrustRank makes a better performance than TrustRank in degrading spam websites or pages. Compared to TrustRank, Topical TrustRank can decrease spam from the top ranked websites by as much as 43.1%. Both TrustRank and Topic TrustRank need seed set selection, and topic TrustRank also needs finding different topics. It is very difficult to gain all the necessary information from a very large network manually in advance, and the size of seed set is also hard to determine. So these methods are not suitable in a large trust network.

Truth discovery is another research involving Credibility Problem. Xiaoxin Yin et al. [21] propose a Truthfinder algorithm to find true facts with conflicting information from different information providers on the network. This approach is applied on certain domain such as book authors and Movie run time. Truthfinder is a fact based search engine, which ranks websites by computing trustworthiness score of each website using the confidence of facts provided by websites. It utilizes the relationships between websites and their information to find the website with accurate information which is ranked at the top. It discovers trustworthy websites better than popular search engines. A new algorithm called Probability of Correctness of Facts(PCF)-Engine [22] is proposed to find the accuracy of the facts provided by the web pages. It uses the Probability based similarity function (SIM), which performs the string matching between the true facts and the facts of web pages to find their probability of correctness. The existing semantic search engines may give the relevant result to the user query, but may not be completely accurate. Their algorithm compute trustworthiness of websites to rank the web pages. Simulation results show that their approach is efficient compared with existing Voting and Truthfinder [21] algorithms. However, these algorithms require to pre-compute the implicit facts in the knowledge base, which is difficult to achieve in large trust networks.

What we present in this paper starts from a unique observation that combining social trust and similarity analysis could benefit each other through information exchange. Credibility Problem is an important research branch on social networks. The task of trust problem is to choose most reliable users in a certain social network [7, 23]. Similarity analysis on social network is usually based on nodes common neighbors or link properties, e.g., [13]. Unlike most of them, we apply more information from social trust side to improve the similarity measure, which is not considered in previous similarity research, such as Reinforced Similarity Integration in Image-Rich Information Networks [24]. And Simrank [25–27] is a famous similarity algorithm in structure network, which is improved in this work.

We have also noticed that there is another work studied a total different relation of social influence and similarity together [12, 28]. They studied how peoples influence and their similarities affect each other. In another word, they consider the same type of nodes similarity and influence in a simple network.

We consider trust of one type of nodes, with the information of similarity of another type of nodes, and vice versa, in a multiple-relational network.

3 Methodology

In this section, we first define the term "credibility" precisely before describing and analyzing an algorithm to compute it. Given a multiple-relational network G_M (e.g., Epinions network as Fig. 2), we present how to convert G_M (only consider trust and rating relations) into two simple graphs $G_T = (V_T, E_T, w_T)$ and $G_S = (V_S, E_S, w_S)$. V and E can be constructed by exploiting one relationship from G_M. For instance, we could construct the vertices and the edges based on the users and their trustiness relationships in Epinions network, respectively. As we discussed in Section 1, the edge weight w can be assigned by analyzing the degree of relation in G_M and the detail is discussed as follows.

3.1 Problem Definition

Formally, let $G = \{V, E, w\}$ be a simple graph, where an edge $e_{ij} \in E$ (directed from node i to node j) has weight $w_{ij} \in [0, 1]$. We say that node i gives the trust-score of w_{ij} to node j.

Let $d^o(u_i)$ denotes the set of all outgoing links from node u_i and likewise, $d^i(u_i)$ denotes the set of all incoming links to node u_i. Credibility of a node is directly proportional to the confidence of all the behaviors provided by it and the implication on it. We firstly introduce one important definition in this paper, the confidence of behavior.

- Confidence of behavior: the confidence of a behavior b (denoted by c(b)) is the probability of b being reliable, according to the best of our knowledge.

Different behaviors about the same object may be conflicting. For example, one user claims that a product is "perfect" whereas another claims that it is "terrible". However, sometimes behaviors may be supportive to each other although they are slightly different. For example, one user claims the product to be "acceptable" and another one claims "not bad" or one user says that a certain mobile phone is 4 inches screen, and another one says 10 cm. If one of such behaviors is reliable, the other is also likely to be reliable. We find that the confidence of behavior is decided by the similarity, so we only consider the similarity to replace the confidence of behavior in the following sections.

Finally, we measure credibility of a node:

- Credibility: This reflects the expected value of each inlink from its neighbor nodes based on their similarities (confidence of their behaviors).

This definition means the credibility of one node depends on its neighbors' credibilities and their similarities. In the next section, we show all steps to calculate the Credibility.

3.2 Trust Similarity

Trust Similarity (TS) network is a special type of heterogeneous network with edge weights of different practical meanings for different edge types. We have noticed that it is generic enough to get important relations for different types of nodes and explore the hidden reinforcement between trust and similarity. Similarity of two nodes in a trust-based network is defined as the summation of similarities between their neighbors. A strong assumption here is that nodes are trusting and trusted by nodes those are similar to them. TS network is a directed multiple-relational network G_M (V, E, w) of two different types of nodes, two types of edges with associated edge features. For ease of presentation, let V_T be the set of nodes we want to study trust on and V_S is the set of the type of nodes for similarity research, where $V = V_T \bigcup V_S$. There are two types of edges E_{TT}, E_{TS} connecting different types of nodes, and $E = E_{TT} \bigcup E_{TS}$. w is a weight vector associated with different types of edges. $w = w_T \bigcup w_S$. $w_T = \{w_T | \forall e_T \in E_{TT}\}$ is a vector of variables, each one of which describes the trust scores between two nodes of an edge e_T. Similarly, $w_S = \{w_S | \forall e_S \in E_{TS}\}$ is another vector of variables for similarity scores on the other type of nodes.

As seen in the above discussion, Fig. 3 and Fig. 4 illustrate the decoupled result of Fig. 2. In the following subsections, we will model the information passing in details in the coordination with the Trust Similarity reinforcement. The similarity of two nodes is the propensity to do the behaviors on other objects. Thus, the propensity or similarity of two nodes can be measured by the difference between the ratings that a node provides to another node. Multiple-relational Network G_M can be converted into two simple G_T and G_S. It is obvious that a higher score similarity of (u_i, u_j) $(Sim^{(\phi+1)}(u_i, u_j))$ implies that the trust relationship of u_i and u_j is more reliable. The similarity of two user nodes u_i, u_j is determined by the similarity in G_T and G_S, using Reinforcement Learning, given by Eq. 1.

$$Sim^{(\phi+1)}(u_i, u_j) = \alpha Sim_T^{(\phi)}(u_i, u_j) + (1-\alpha) Sim_S^{(\phi)}(u_i, u_j) \tag{1}$$

Where α is a parameter, which is used to weigh the importance of two similarities.

In Trust network like Fig. 3, a user's similarity depends on its neighbors [27], user tends to trust similar users like him, in other words, user's trust similarity $(Sim_T^{(\phi+1)}(u_i, u_j))$ is determined by his inlinks and outlinks, which can be calculated by Eq. 2.

$$\begin{aligned} Sim_T^{(\phi+1)}(u_i, u_j) = & \frac{\beta}{|d^i(u_i)||d^i(u_j)|} \sum_{u_p \in d^i(u_i)} \sum_{u_q \in d^i(u_j)} Sim_S^{(\phi)}(u_p, u_q) \\ & + \frac{1-\beta}{|d^o(u_i)||d^o(u_j)|} \sum_{u_p \in d^o(u_i)} \sum_{u_q \in d^o(u_j)} Sim_S^{(\phi)}(u_p, u_q) \end{aligned} \tag{2}$$

Here, β is a parameter, which determining the weight of inlinks and outlinks in G_T.

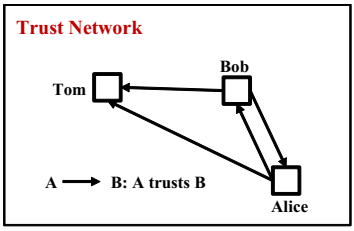


Fig. 3. An Example of Trust Network

In Epinions network, the similarity of two users can be viewed as their ratings on different products. For the sake of calculation, we simply transform the rating graph G_S into a bipartite graph $G_b = (V_1, V_2, E_b)$, where V_1 and V_2 represent two different types of objects. As shown in Fig. 4, V_1 represents a set of users (u_x) and V_2 represents a set of products (o_y) in Epinions. Given such a bipartite graph, we can compute the similarity score for each pair of objects of the same type using Simrank++ [26], which is based on the underlying idea that two objects of one type are similar if they are related to similar objects of the second type. Formally, the similarity score in Simrank++ is computed by the following equations.

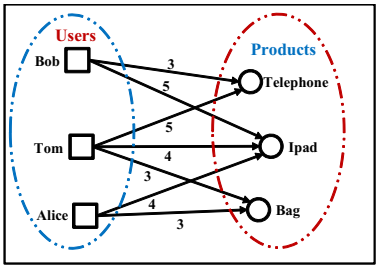


Fig. 4. An Example of Users-Products Bipartite Graph

$$Sim_S^{(\phi+1)}(u_i, u_j) = evidence(u_i, u_j) \cdot \Theta_1 \cdot \sum_{(u_i,o_i)\in E_b} \sum_{(u_j,o_j)\in E_b} \mathbf{W}(u_i, o_i)\mathbf{W}(u_j, o_j) Sim_S^{(\phi)}(o_i, o_j) \tag{3}$$

$$Sim_S^{(\phi+1)}(o_i, o_j) = evidence(o_i, o_j) \cdot \Theta_2 \cdot \sum_{(o_i,u_i)\in E_b} \sum_{(o_j,u_j)\in E_b} \mathbf{W}(o_i, u_i)\mathbf{W}(o_j, u_j) Sim^{(\phi)}(u_i, u_j) \tag{4}$$

Where Θ_1 and Θ_2 are constant. $evidence(x, y)$ and $\mathbf{W}(x, y)$ are defined as follows.

$$evidence(x, y) = \sum_{i=1}^{|N(x)\cap N(y)|} \frac{1}{2^i} \tag{5}$$

Where $|N(x) \cap N(y)|$ denotes the common neighbors between x and y.

$$\mathbf{W}(x,y) = e^{-variance(y)} \cdot \frac{w(x,y)}{\sum_{(x,z)\in E_b} w(x,z)} \tag{6}$$

Where $variance(y)$ is the variance of the weight of edges that are connected to the node y.

3.3 Credibility

The credibility value of a node represents the true trust of a node. We can use credibility to define true trust. Credibility is the expected value of an incoming link from a reliable node. The credibility value depends on the quality of the inlinks, and not only the quantity: credibility of a node with one high quality inlink is equivalent to a node with many high quality inlinks. This definition differs from the usual random-walk based methods where the number of inlinks matter. For each inlink, we remove the effect of unreliability from the weight and then we compute the mean of all inlinks. The credibility of a node i is given by Eq. 7.

$$Credibility(u_i) = \sum_{u_p \in d^i(u_i)} \frac{Sim(u_p, u_i)}{\sum_{u_q \in d^o(u_p)} Sim(u_p, u_q)} w_{u_p u_i} \tag{7}$$

The credibility value lies in the range [0, 1].

4 Experiment

In this section, we conduct different kinds of experiments to evaluate and analyze our algorithms on the real-world social network.

4.1 Datasets

In our experiment, we apply two real datasets (Epinions and DBLP). The Epinions data are crawled from Epinions.com until April 2010. The three relations in Epinions are, 1) users can trust other users; 2) users can post a review with product rating (from star 1 to star 5) about one product belonging to a certain category; 3) people can vote (very helpful, helpful, somewhat helpful, not helpful and off topic) for someone's review. In this evaluation, we only consider the trust relation and rating relation between users in Epinions. The multiple-relational network can be shown as Fig. 2. And the DBLP data are available from the Citation Network Dataset (http://arnetminer.org/citation). There are two relations in DBLP, 1) coauthor relation; 2) citation relation. The multiple-relational network can be described as Fig. 5. Table 2 shows the various classes of statistics about the two datasets.

In a small graph, we can expect a high credibility value of a node, while the connections are much reasonable. For example, consider a pair of nodes with just

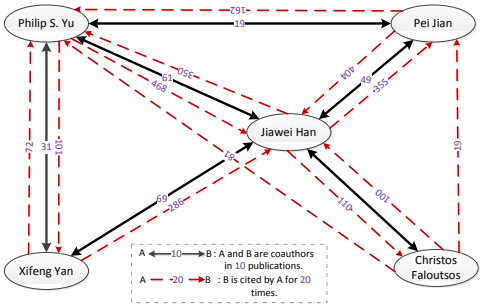


Fig. 5. An Illustration of Multiple-Relational Network of DBLP

Table 2. Detail of Dataset

Dataset	Epinions		DBLP	
	Trust	Rating	Coauthor	Citation
Nodes	98027	273437	595561	116667
Edges	612452	1076051	1311712	500000
Avg. of Degree	6.2478	3.9353	2.2025	4.2857

one directed edge. It is easy to see whether the reliability of one undefined node is reasonable from the other nodes. Similarly, the credibility of one undefined node will be the summation of each edge weight from the other nodes. While random-walk based techniques will give low scores to nodes in such components due to their low connectivity, in our model, they may get high credibility value based on the same connectivity. However, in general, credibility values do not make much sense if the graph is very small.

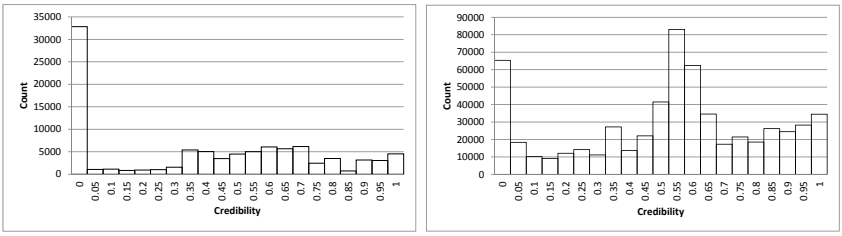
4.2 Distribution of Credibility

The first set of experiments measure the distribution of credibility values of the nodes. Fig. 6 shows the chart of the credibility value for both the datasets. In both datasets, count of nodes with credibility as 0.6 is very high.

However, the distribution of credibility is smoother due to the removal of the effect of unreliability, especially for Epinions. For DBLP, the distribution is not so smooth because of the presence of too many disconnected components in small size. In such small sized graphs, as previously discussed, if the degree is 1 or 2, the credibility values become close to that as well.

4.3 Comparison of Credibility with Ranking

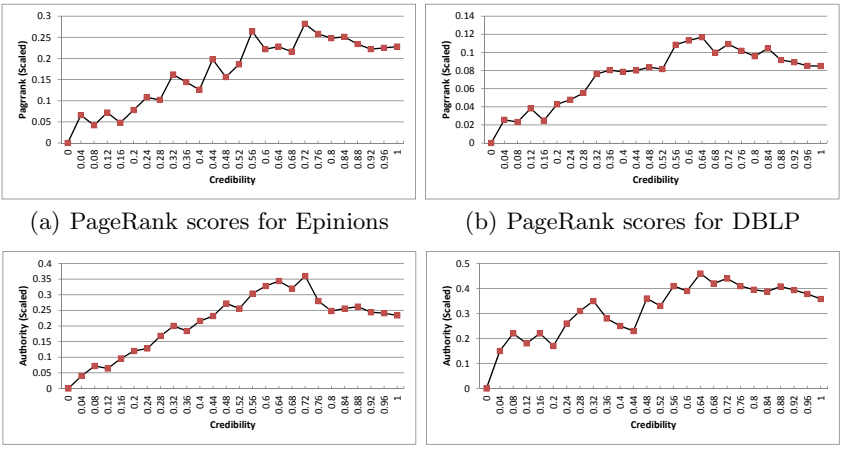
The next set of experiments compare the ranking of nodes using the credibility values against that produced by the popular ranking algorithms such as PageRank [3] and HITS [2].



(a) Distribution of credibility for Epinions (b) Distribution of credibility for DBLP

Fig. 6. Distribution of credibility for two Datasets

Fig. 7 shows the comparison. Note that we have scaled the PageRank and HITS score by multiplying with 1000. One common trend we observe is that nodes with less credibility have low HITS and PageRank score, and those with high credibility have high score. This shows that the ranking determined by the credibility values conform to the perception that more popular nodes have more credibility.



(a) PageRank scores for Epinions (b) PageRank scores for DBLP

(c) HITS authority scores for Epinions (d) HITS authority scores for DBLP

Fig. 7. Comparison of credibility with ranking

However, towards the end (when credibility is also almost equal to 1), there is a drop in the scores. This is partly due to our model. Even if a node has few connections but has a high quality inlink, it will attract high reputation. The same is not true for the other two algorithms. Moreover, the two datasets have a large number of strongly connected components and most of them are very small in size. The nodes in these small components have high credibility, but due to their small sizes, they have low scores.

4.4 Connection to Balance Theory

In this evaluation, our method conforms to balance theory. The balance theory includes (i) "a friend's friend is a friend", (ii)"an enemy's friend is an enemy", (iii)"a friend's enemy is an enemy" and (iv) "an enemy's enemy is a friend". More information of balance theory can be found in [12–15].

Assume S is the set of all occurrences of the pattern $i \to j \to k$ where the direct link $i \to k$ exists. We compute the error using the following equation as [16]:

$$\delta = \frac{1}{4|S|} \sum_{\{i,j,k\} \in S} (w_{ij} w_{jk} - w_{ik})^2 \tag{8}$$

Here, the number 4 in the denominator is a normalizing constant.

In this assessment, we evaluate our model with the balance theory. Initially, we compute the conformity of the graph using Eq. 8 on the original network. Secondly, we compute the error removing the bias from each edge as [16]. Finally, we remove unreliability from each edge using Eq. 7, and re-compute the error.

Table 3. Error of conformity with balance theory

Relationship	Epinions			DBLP		
	δ_o	δ_b	δ_u	δ_o	δ_b	δ_u
friend-friend-friend	0.03	0.03	0.03	0.04	0.05	0.04
friend-enemy-enemy	0.55	0.43	0.37	0.61	0.49	0.42
enemy-friend-enemy	0.38	0.34	0.29	0.33	0.28	0.25
enemy-enemy-friend	0.62	0.41	0.27	0.48	0.35	0.22

Table 3 shows the errors of two datasets. Here, δ_o shows the error of the original graph, δ_b shows the error after removing bias [16] and δ_u shows the error after removing unreliability. Our method almost improves the result except in the case of "a friend's friend is a friend" where the error is a small value. Thus, we can conclude that considering the credibility of a node and utilizing it benefits the conformity of the balance theory in the network.

4.5 Case Study

In the final experiment, we want to compare the scores computed by three different algorithms including PageRank (PR), HITS and Credibility (Cred.) for top-10 reliable users from Epinions and DBLP. We select Top-10 reviewers for the most popular authors overall provided by Epinions, and we select Top 10 researchers with highest H-Index in DBLP. In Table 4, we can find that our method produces a better result than others. The credibility scores conform to the manual ranking. PageRank and HITS scores in Table 4 is multiplied by 1000.

Table 4. Top-10 Users' Different Scores in Epinions & DBLP

Epinions				DBLP			
Name	PR	$HITS$	$Cred.$	Name	PR	$HITS$	$Cred.$
jo.com	0.2798	0.3553	0.7431	Herbert A. Simon	0.1183	0.4525	0.6714
dkozin	0.2251	0.3147	0.7251	Anil K. Jain	0.0852	0.4042	0.6542
mkaresh	0.2342	0.3341	0.7209	Scott Shenker	0.0913	0.4228	0.6173
Freak369	0.2739	0.2324	0.7123	Terrence Sejnowski	0.0964	0.3805	0.6065
Bryan_Carey	0.1951	0.3027	0.7037	Hector Garcia-Molina	0.1002	0.4149	0.6042
three_ster	0.2031	0.2232	0.6725	Takeo Kanade	0.0722	0.3623	0.5937
shoplmart	0.2594	0.1851	0.6328	Jiawei Han	0.0773	0.3774	0.5861
dlstewart	0.2161	0.2331	0.6074	Tomaso Poggio	0.0817	0.3811	0.5431
Howard_Creech	0.1973	0.1927	0.5596	Philip S. Yu	0.0753	0.3626	0.5135
ChrisJarmick	0.1912	0.2198	0.5284	David Haussler	0.0761	0.3341	0.4912

5 Conclusion

We observe the benefits of modeling trust and similarity together for ubiquitous multiple-relational network. We design a method to model and demonstrate the advantages for both sides using a large scale real world data. We believe that analysis on multiple-relational network has a bright future because social trust and similarity studies are two building blocks for many research interests, such as ranking, clustering, classification and recommendation. For many applications involving trust-based networks, it is crucial to assess the credibility of a node. In this paper, we have proposed an algorithm to compute the credibility of nodes in networks where the edge weight denotes the trust score, using the similarity of nodes in Reinforcement Learning. The experiment result shows that our algorithm significantly improves the performance than others'. Our model conforms well to other graph ranking algorithms and social theories such as the balance theory. However, our algorithm may be misguided by malicious nodes and plotting groups. In the future work, we would like to deal with these problems and other malicious attacks. Moreover, we will explore a distributed application of our approach.

Acknowledgement. The work was supported in part by Fund of Science and Technology Development of Macau Government under FDCT/106/2012/A3 and by University Macau Research Committee under MYRG188-FST11-GZG.

References

1. International, P.S.R.A., WebWatch, C.R.: Leap of Faith: Using the Internet Despite the Dangers: Results of a National Survey for Consumer Reports WebWatch. Consumer Reports WebWatch (October 2005)
2. Kleinberg, J.M.: Authoritative sources in a hyperlinked environment. J. ACM 46(5), 604–632 (1999)
3. Page, L., Brin, S., Motwani, R., Winograd, T.: The pagerank citation ranking: Bringing order to the web. Technical report, Stanford InfoLab (November 1999)
4. Braunstein, A., Mézard, M., Zecchina, R.: Survey propagation: an algorithm for satisfiability. CoRR cs.CC/0212002 (2002)

5. Sherchan, W., Nepal, S., Paris, C.: A survey of trust in social networks. ACM Comput. Surv. 45(4), 47 (2013)
6. Orman, L.V.: Bayesian inference in trust networks. ACM Trans. Manage. Inf. Syst. 4(2), 7:1–7:21 (2013)
7. Bonacich, P.: Factoring and weighting approaches to status scores and clique identification. The Journal of Mathematical Sociology 2(1), 113–120 (1972)
8. Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In: WWW, pp. 640–651 (2003)
9. Richardson, M., Agrawal, R., Domingos, P.: Trust management for the semantic web. In: Fensel, D., Sycara, K., Mylopoulos, J. (eds.) ISWC 2003. LNCS, vol. 2870, pp. 351–368. Springer, Heidelberg (2003)
10. de Kerchove, C., Dooren, P.V.: The pagetrust algorithm: How to rank web pages when negative links are allowed? In: SDM, pp. 346–352 (2008)
11. Guha, R.V., Kumar, R., Raghavan, P., Tomkins, A.: Propagation of trust and distrust. In: WWW, pp. 403–412 (2004)
12. Cartwright, D., Harary, F.: Structural balance: A generalization of heider's theory. Psychological Review 63(5), 277–293 (1956)
13. Heider, F.: Attitudes and cognitive organization. J. Psychology 21, 107–112 (1946)
14. Leskovec, J., Huttenlocher, D.P., Kleinberg, J.M.: Signed networks in social media. In: CHI, pp. 1361–1370 (2010)
15. Leskovec, J., Huttenlocher, D.P., Kleinberg, J.M.: Predicting positive and negative links in online social networks. In: WWW, pp. 641–650 (2010)
16. Mishra, A., Bhattacharya, A.: Finding the bias and prestige of nodes in networks based on trust scores. In: WWW, pp. 567–576 (2011)
17. Li, R.H., Yu, J.X., Huang, X., Cheng, H.: A framework of algorithms: Computing the bias and prestige of nodes in trust networks. CoRR abs/1207.5661 (2012)
18. Koutra, D., Ke, T.-Y., Kang, U., Chau, D.H(P.), Pao, H.-K.K., Faloutsos, C.: Unifying guilt-by-association approaches: Theorems and fast algorithms. In: Gunopulos, D., Hofmann, T., Malerba, D., Vazirgiannis, M. (eds.) ECML PKDD 2011, Part II. LNCS, vol. 6912, pp. 245–260. Springer, Heidelberg (2011)
19. Gyöngyi, Z., Garcia-Molina, H., Pedersen, J.O.: Combating web spam with trustrank. In: VLDB, pp. 576–587 (2004)
20. Wu, B., Goel, V., Davison, B.D.: Topical trustrank: using topicality to combat web spam. In: WWW, pp. 63–72 (2006)
21. Yin, X., Han, J., Yu, P.S.: Truth discovery with multiple conflicting information providers on the web. IEEE Trans. Knowl. Data Eng. 20(6), 796–808 (2008)
22. Srikantaiah, K.C., Srikanth, P.L., Tejaswi, V., Shaila, K., Venugopal, K.R., Patnaik, L.M.: Ranking search engine result pages based on trustworthiness of websites. CoRR abs/1209.5244 (2012)
23. Golub, G.H., Van Loan, C.F.: Matrix computations, 3rd edn. Johns Hopkins University Press, Baltimore (1996)
24. Jin, X., Luo, J., Yu, J., Wang, G., Joshi, D., Han, J.: Reinforced similarity integration in image-rich information networks. IEEE Trans. Knowl. Data Eng. 25(2), 448–460 (2013)
25. Zhao, P., Han, J., Sun, Y.: P-rank: a comprehensive structural similarity measure over information networks. In: CIKM, pp. 553–562 (2009)
26. Antonellis, I., Garcia-Molina, H., Chang, C.C.: Simrank++: query rewriting through link analysis of the click graph. PVLDB 1(1), 408–421 (2008)
27. Jeh, G., Widom, J.: Simrank: a measure of structural-context similarity. In: KDD, pp. 538–543 (2002)
28. Wang, G., Hu, Q., Yu, P.S.: Influence and similarity on heterogeneous networks. In: CIKM, pp. 1462–1466 (2012)