Towards trust inference from bipartite social networks

Daire O'Doherty
Universite catholique de Louvain
1348 Louvain-La-Neuve, Belgium
daire.odoherty@student.uclouvain.be

Salim Jouili
EURA NOVA
Rue Emile Francqui, 4
1435 Mont-Saint-Guibert, Belgium
salim.jouili@euranova.eu

Peter Van Roy
Universite catholique de Louvain
1348 Louvain-La-Neuve, Belgium
peter.vanroy@uclouvain.be

ABSTRACT

The emergence of trust as a key link between users in social networks has provided an effective means of enhancing the personalization of on-line user content. However, the availability of such trust information remains a challenge to the algorithms that use it, as the majority of social networks do not provide a means of explicit trust feedback. This paper presents an investigation into the inference of trust relations between actor pairs of a social network, based solely on the structural information of the bipartite graph typical of most on-line social networks. Using intuition inspired from real life observations, we argue that the popularity of an item in a social graph is inversely related to the level of trust between actor pairs who have rated it. From an existing bipartite social graph, this method computes a new social graph, linking actors together by means of symmetric weighted trust relations. Through a set of experiments performed on a real social network dataset, our method produces statistically significant results, showing strong trust prediction accuracy.

Categories and Subject Descriptors

H.3.3 [**Information Storage and Retrieval**]: Information Search and Retrieval—*information filtering, Selection process, Retrieval Models*; I.5.1 [**Computing Methodologies**]: Pattern recognition—*Models*

General Terms

Algorithms

Keywords

Social network, Trust inference, Bipartite graph, Social Trust, Vertex similarity

1. INTRODUCTION

The exponential growth and development of Web 2.0 has brought about a rapid increase in the availability of on-line user content, as well as creating a fundamental shift in the way people use, and share knowledge. The popularity and increased usage of blogs and wikis have given rise to new means of on-line collaboration and information sharing, and have created a virtual platform in which users can explicitly express their preferences, and opinions. Furthermore, the emergence of social networks has allowed users to connect themselves to any number of people they know, or who share these preferences and perspectives, forming vast on-line communities of similar, like-minded users. The Internet, as such, has itself become a large social network, linking "people, organizations and knowledge" [3]. With such a vast and ever increasing availability of knowledge and content, these developments have pushed researchers to develop techniques to handle this *information overload*, and to provide certain forms of personalization of the information and content, that would be of the most interest to each individual user. One ongoing area of research attempting to fulfill these needs, is that of the incorporation of *trust* into on-line systems.

The emergence of trust [20, 11, 25, 19] as a key link between users in social networks is a growing area of research, where trust has been used for the improvement and enhancement of the individual personalization of many on-line activities. In particular, many studies [12, 5, 23, 25] have shown trust to be greatly effective in improving the relevance and scalability issues of traditional recommendation techniques, as well as reputation systems for on-line peer-to-peer file sharing [14]. Such research is based on the sociological idea that users are more inclined to have similar opinions to people that they know and trust. For the purposes of this investigation, we follow the notion of trust as an indication of similarity or commonality between two users in a network. More formally, a trust metric from user u to user v in a social network can be seen as the subjective probability that the truster, u will have the same preferences and tastes as the trustee v.

However, although trust has been shown to improve content personalization and the clustering of similar users [24, 27, 26, 8], it is necessary to be able to effectively and efficiently obtain accurate trust information for use in such systems. Some previous studies [10, 18] have made use of explicit user trust assertions as a means for providing such enhancements. Potential drawbacks of this reliance on explicit user feedback include its unavailability as well as its unreliability. The unreliability of this feedback may be caused by the potential reluctance of users to publicly provide such feedback, as well as potential user indifference to the system, presenting inconsistencies in the provided trust metrics, which may negatively impact the success and appropriateness of the systems using them. The unavailability of such explicit feedback is also due to the fact that many social networks do not provide the means for this kind of explicit feedback. Taking a real world example of the popular social network Youtube.com, an on-line medium for the distribution of videos, users are able to individually contribute and watch videos, as well state personal preferences by either rating videos or subscribing to different groups. In essence, this network represents a bipartite graph with two distinct sets of vertices, namely users and videos. The edges in the graph represent explicit user preferences for videos in the form of ratings or subscriptions to particular groups. However, this site, like many of its type, does not provide any mechanism for explicit user to user connections, such as a trust connection that may be used for the enhancement of the individual user experience.

Based on real life observations, we are interested in investigating how we can automatically infer trust connections between users based on the correlation of user similarity and trust [30, 9, 29] in a social network. In order to provide a generic methodology applicable to all social graphs, we aim to use only the information contained in the topology and structure of the bipartite graph itself, namely the directed edges from user vertices to items, and not to use any of the content of the graph, as such content is individual to each social network. Using this information, we distinguish and base our work on the items for which a pair of users both have a directed edge.

2. PROBLEM FORMULATION

Previous studies have shown many benefits of trust in the context of social networks and content recommendation. Trust has been shown to provide a more accurate solution to content recommendation, as well as providing a much needed robustness to malicious users [14]. With such advantages, it is clear that the availability of such connections is invaluable to the enhancement of on-line social recommendation systems and on-line user experience in general.

Traditionally, recommendation systems [1, 22] deal with a bipartite graph representing a set of actors (e.g. users) connected to a set of items (e.g. books). Each connection corresponds to an act through which an actor performs an operation on an item (rating, buying, commenting…). Formally, let $G = (A \cup I, E)$ be a bipartite graph where A and I are two disjoint sets, the set of $actor$ and the set of $item$ vertices respectively, and $E \subseteq A \times I$ is the set of edges (i.e. interactions between actors and items). The difference with a classical graph lies in the fact that edges only exist between actor vertices and item vertices. Recommendation algorithms aim to predict a set of edges $e \in E$ that are *relevant* to the individual actors. Trust aware social recommendation provides a prediction by means of the trust information between actors, consisting of a set of relations between actors within the set A. As stated above, this trust information is most often provided through explicit feedback from actors in only a few on-line social networks, with the large majority of social networks not explicitly providing such functionality. In this work, we aim to provide a measure that computes the trust between actors based on the whole bipartite graph. Formally speaking, from a bipartite graph $G = (A \cup I, E)$ describing interactions between actors and items, we want to create a graph $\mathbf{g} = (A, T)$ where A is the set actor vertices and $T \subseteq A \times A$ is the set of edges representing the trust relations between actors.

Previous studies [17, 7, 28, 6] have been made to predict such trust relations based on probabilistic models. However, to the best of our knowledge, no algorithm exists that allows for the automated inference of such trust based solely on the topological information of a bipartite graph. Our investigation is thus motivated by the need of an automated and generic method for the inference of trust connections between actors in social graphs. We aim to provide trust metrics fit to be used by trust aware algorithms that have been designed to enhance on-line user experience, such as trust aware social recommendation systems, allowing their application without the need for explicit user feedback, nor the use of any content of the graph, as such content can differ depending on the network.

3. TRUST INFERENCE

Based on intuition inspired from real life observation, in this section we present our methodology for the inference of trust relations between users in a social graph. Following this, we then introduce and explain our chosen formula based on the described methodology used for the implementation of this trust inference and the construction of a new trust graph connecting users, from structural information present in a social bipartite graph.

3.1 A Methodology for Inference of Trust

To infer trust connections between two actors in a social network, our work is concentrated solely on the topological and structural information present in the social bipartite graph presented above. From this information, we focus our investigation on the common relationships between vertices in set A to set I. For a social bipartite graph consisting of two distinct sets of vertices, set A and I , as described above, we define a *shared item* between two vertices in A to be any vertex in set I for which both vertices in set A have a directed edge. Our work distinguishes these *shared items* according to their relative *popularity* in the graph, which we define as the indegree of this item, or the number of directed edges from vertices in set A to this vertex in I. Based on real life observations, our work follows the intuition that: the higher the indegree of a vertex in set I, the *less* we can deduce about the similarity between two vertices in A who both have a directed edge to this vertex , and thus, the less we can say about the potential trust relationship between them. This intuition is inspired from our real life observations of the popularity of items and people in a social context. Considering a real life example of the book "Harry Potter", which has been the subject of widespread popularity and attention for more than a decade, if two users of a social network such as "*AllConsuming.net*", where users can rate and review books, were to provide a positive rating for Harry Potter, we argue that there is little that we can deduce about their relative similarity, as the approval of such a popular and widely known book may well be partially due to the popularity and widespread appeal of the book in general and does not constitute a distinguishing character trait.

However, we do not limit this intuition solely to books or items. If we were to take the "follows" graph of the social network "*twitter.com*", we can consider a famous singer or actor and apply the same intuition. For example, the English actor Stephen Fry is a popular and well known public figure, who happens to be an avid user of twitter. At the time of the writing of this paper, he has 3,995,447 followers on this social network. From our intuition, we argue that there is little we can deduce about the similarity or potential trust connection between two users of twitter who both "happen" to follow Stephen Fry. As before, such a connection is more likely to be based on the popularity of the public figure more than a strong similarity or character trait between the two followers. Following the same methodology, and based on the proposed correlation of user similarity and trust [30, 9, 29], we state that the lower the indegree of a vertex in I, meaning the less popular a particular item is in the graph, the *more* we can deduce about the similarity between two vertices of set A who have an edge to this vertex, and thus, the probability that they will have similar tastes will be greater. As such, a connection is more likely to be based on a genuine interest in such item and not on coincidence or popularity of the item itself.

Further to this intuition, we also take into account the concept that trust can be built through other means within social networks. To take a concrete example common to most social networks, users may access publicly available comments from other users in the network and may agree or disagree, thus a user may subsequently trust the user who issued this comment directly through such means with a certain probability. This is also taken into account in our inference of trust, as will be seen.

3.2 Deriving a Formula for Trust Inference

Building upon the methodology of *shared items* presented above, we believe that there are two main structural factors that need to be taken into account in order to infer trust connections between two users in our social bipartite graph. Firstly, we believe that it is necessary to take into account the *Relative Diversity* between the two users, which we define as the number of neighbours that both users can reach through two hops in the graph. Using only the topological information of the graph, we follow the approach of *structural similarity* as presented in [15], using the *Jaccard Index* to compute a distance measure between vertices in set A based on the neighbourhood of each vertex. As we are dealing with a bipartite graph, each vertex does not have a direct connection to a vertex in the same set. We thus consider the neighbourhood of a vertex $u \in A$ as the set of vertices $S \in A$ through which vertex u has an indirect connection in the graph through the vertices in set I for which u has a directed edge. We define this as the *two-hop neighbourhood* of u, connecting u to vertices in the same set, through $u's$ interaction with vertices in set I. To compute this relative diversity between two vertices u and v, we thus consider both of their two-hop neighbourhoods as two sets, and we apply the *Jaccard Index* between these sets. The Jaccard index [13] is a well known statistic, widely used to compare the similarity and diversity of sample sets and perfectly suits our need to compute the relative diversity between two vertices in our bipartite graph. This formula is presented below in equation 1 , where N_u represents the neighbourhood of vertex u and N_v represents the neighbourhood of vertex v.

$$J(u,v) = \frac{|N_u \cap N_v|}{|N_u \cup N_v|} \tag{1}$$

The second structural factor we believe to contribute to social trust is that of our intuition of shared items presented above. Based on this intuition, we need to provide the distance between two vertices in set A in relation to the *popularity* of the vertices in set I for which they both have a directed edge. The formula used to compute this distance value based of shared vertices is presented in equation 2, where $deg(i)$ represents the indegree of item i. The more highly connected a shared vertex, the higher the resulting distance value will be, and consequently, the less connected a shared vertex is, the lower the distance value will be. Thus, this equation rewards low connected shared items, and penalizes highly connected shared items.

$$D(i) = (\frac{2}{1 + e^{(-deg(i)^{\sigma} + 2^{\sigma})}} - 1) \tag{2}$$

Figure 1 shows the behavior of this formula as a function of the degree of an item and the constant parameter σ. As we can see from this curve, as the degree of the item i increases, the output value $D(i)$ also increases exponentially. This perfectly fits our methodology of rewarding low connected items while penalizing highly connected items. The resulting values $D(i)$ are normalized in the interval $[0,1]$. Moreover, the parameter $0 < \sigma < 1$ is incorporated to the equation in order to provide a way to adjust the slope of the curve. Concretely, this parameter allows to modify the distribution of the values $D(i)$ over $[0,1]$. In practical terms, the increase of σ causes $D(i)$ to rapidly reach high values, meaning that in the case of $\sigma = 0.8$, when the degree of the item is near to 10, the computed $D(i)$ values will be very near to 1. However, in the case of $\sigma = 0.2$, the $D(i)$ values reach 1 with items having degrees ≥ 1000. In other words, this parameter is used to define from which degree value an item is considered as popular. This will depend on the data sets involved. In addition, the minimum value 0 of $D(i)$ is obtained when the degree of the involved item is set to two, whatever the value of σ. In practical terms, this corresponds to the case where an item is only rated by the users involved in the computation themselves. By combining these two aspects, both the relative diversity and the distance based on shared vertices, our trust inference formula is presented as a whole in the below equation 3.

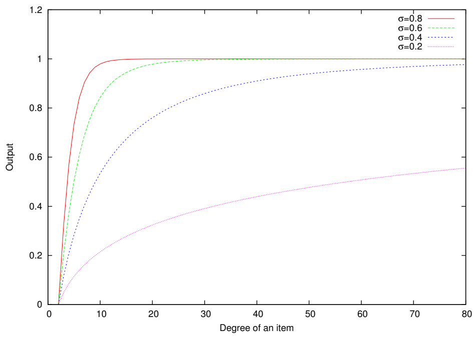


Figure 1: Formula for Shared Items

$$Trust(u,v) = \alpha + \beta J(u,v) + \gamma(1 - \frac{\sum_i^{i \in SI} D(i)}{|SI|}) \tag{3}$$

where SI is the set of shared items between the users involved, and $\alpha + \beta + \gamma = 1$. The constant α defines the probability that a pair of users trust each other through any other form of external information (i.e. recommendation, search engine . . .). This parameter is inspired by the "teleportation" parameter used in the PageRank algorithm [4, 21] which defines the probability of the direct access to a web page (without following hyperlinks). The constants β and γ define the contribution of each proposed factor to the computation of the trust between a pair of users.

4. EXPERIMENTAL EVALUATION

4.1 Data set

In order to test our methodology we needed to be able to compare the results of our tests against meaningful real life trust assertions. For this, we needed real life test data consisting of:

1. A real life social bipartite graph containing two sets of vertices, A and I, representing a set of actors, and a set of items respectively. This graph should also contain directed edges from actor vertices in set A to item vertices in set I, representing explicit ratings of items by users. This graph, hereon referred to as the *ratings graph* , will be used for the application of our trust inference formula.

2. A corresponding real life social trust graph, containing explicit trust assertions between the user vertices in set A. This trust graph must belong to the same social network and be complementary to the ratings graph.

For the purposes of our experiments we used the *epinions* dataset available from trustlet.org. Epinions.com is an on-line social network where users contribute reviews and share their opinions on any number of items or topics, from books and DVDs to holidays and restaurants. Users can also provide ratings on a scale of 1 to 5 for these items. In addition to this rating system, epinions also provides a "*Web Of Trust*" facility, whereby users can explicitly provide "*trust*" assertions, indicating their individual trust for other users in the network. These ratings, as well as the web of trust service are used to provide recommendations for item reviews deemed to be most applicable to individual users. Importantly, these ratings are also used to designate the top ranked reviews for each item. The more highly rated a review is, especially if these reviews are provided by highly trusted users, the more prominent position this review will take.

This dataset provides all aspects of a dataset necessary to evaluate our methodology. *Epinions* is also a well known dataset and has been used in numerous previous studies [11, 19] using trust. One drawback of the use of the trust graph of this dataset, is that the trust assertions it contains do not provide any weight of trust between users on any scale, and indeed do not provide any information of possible "distrust" between users, whereby a particular user may explicitly not like or not trust another user in the network. The trust assertions can be seen as simple directed edges between users, where the existence of an edge indicates a trust assertion from one user to another, while the absence of an edge does not indicate whether these users explicitly do not trust each other, or if these users have not yet come into contact in the graph, or indeed if these users have just failed to provide any explicit feedback to the system.

4.2 Setup

For the remainder of the paper, we consider the ratings graph of the epinions dataset to be a bipartite graph $G = (A \cup I, E)$, with vertices in set A representing the users of epinions and the vertices in set I representing the items of the dataset, and $E \subseteq A \times I$ representing the edges of ratings of items in I from users in A. To set up our test data, we first removed all users in the trust graph that had not rated any items in the corresponding ratings graph. These users are not essential to our experiment and they go against the intuition of shared items behind our methodology. This elimination however had almost no effect on the experiments, as the number of users who had not rated any items was insignificant. We then split our experiments in two: a training and validation phase, and a comparison phase whereby we compare our approach to a naive approach based loosely on the structural methodology.

Firstly, for the validation phase, we followed a classical *holdout* style validation and applied our formula on an independent training set to create a new trust graph, consisting of generated trust links between the users. By comparing the resulting weighted edges of the generated trust graphs computed from the formula with the corresponding real trust assertions provided in the real epinions trust graph we were able to determine local optimal values of each of the parameters of our formula and validate our formula along two key axes as will be explained. In the comparison phase, we first compare our method of trust inference against a similar but naive trust inference method which is loosely based on the same methodology. Following this comparison, we analyze the structural properties [2, 16] of the computed trust graph and compare them to the corresponding properties of the real trust graph of the epinions dataset. We base this comparison on the degree distribution, hop plot, and the clustering coefficient properties of the graphs.

Table 1: Selected parameters

α	β	γ	σ
0.2	0.3	0.5	$\frac{1}{3}$

4.3 Validation

The aim of the validation phase was to both validate our methodology, as well as to optimize the parameters of our chosen trust inference formula. For this, we needed to discover the relative contribution of each aspect of the formula (Eq. 3) to the overall accuracy of the inferred trust graph. Firstly, we chose the value of parameter $\sigma = \frac{1}{3}$, as this value gave us a balanced distribution of the resulting metrics for this dataset, making sure that the metrics did not increase too quickly for items with an average indegree, but are also in line with our methodology of penalizing highly connected items. This, of course, would depend on the database in question, and may indeed change over time. Using a classical *holdout method* of validation, we split the ratings dataset into two independent subsets, the training set, and the test set. We then used the training set to apply our formula and compute the trust links between each user, and thus observed the effect on the resulting computed trust metrics in the generated trust graph by comparing these metrics to the corresponding edges in the real trust graph provided with the epinions dataset. Repeating this step, applying different weights to the different aspects of the formula allowed us to retrieve local optimal values of the parameters α, β and γ. As the edges of the epinions trust graph only indicated the existence of trust or not, and did not provide any scale of the level of trust, we chose a threshold for this comparison to indicate whether the computed trust metrics were to be considered as a trust of not. If the weight of a computed trust edge was less than this threshold, this edge was considered to indicate no trust, and thus if the weight was greater than or equal to the threshold, this edge was considered to be a trust edge.

From this comparison, we validated our formula by computing the number of *true positives (TP)*, as the number of edges in the computed trust graph considered to indicate trust, corresponding to an existing trust assertion edge in the real trust graph, *false positives (FP)* as the number of edges in the computed trust graph considered to indicate trust, but where no corresponding trust edge existed in the real trust graph, *true negatives (TN)* as the number of edges correctly computed to represent no trust assertion in the real graph, and finally *false negatives (FN)* as the number of edges considered to indicate no trust, but where a corresponding trust assertion existed in the real trust graph. Taking measurements inspired from the domain of *information retrieval*, we thus calculated the following metrics:

- **Trust prediction rate**: the fraction of the real trust assertions in the graph correctly identified, as the number of true positives divided by the sum of the number of the true positives and the number of false negatives: $(\frac{TP}{TP+FN})$

- **Distrust prediction rate**: The fraction of correctly predicted distrust assertions, or the number of metrics computed to indicate the lack of trust in the real graph, as the number of true negatives (TN) divided by the sum of the number of true negatives and the number of false positives: $(\frac{TN}{TN+FP})$.

Table 1 illustrates the selected parameters resulting from the validation and training phase. We remark that the $D(i)$ term in Eq. 3

which is related to the shared items has the most important contribution to our trust computation. This validates our intuition based on the fact that the popularity of the shared items has an important impact on the trust between the users involved in the trust calculation.

4.4 Comparison to a Naive Approach

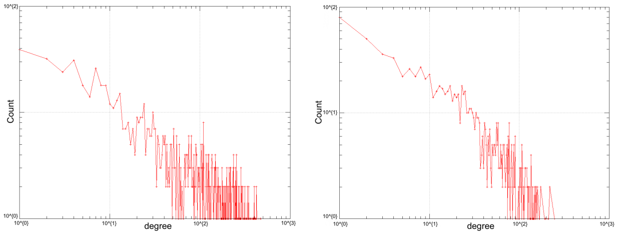
To the best of our knowledge, no other method exists for the inference of trust based solely on the structural information of a social bipartite graph. As a result, to compare the performance of our formula to a similar methodology, we compare our method to a naive trust inference method which also uses only the structural information of the graph, as well as the concept of shared items, and which is also based on the correlation of trust and user similarity.

Based on the underlying nature of many current collaborative filtering recommendation systems, as well as the correlation of similarity and trust proposed in [30, 9] the corresponding naive methodology states that users with similar tastes will have rated the same items, and thus users with shared items should trust each other. Using this methodology, the method infers trust between user pairs if they have both rated at least one of the same items. Table 2 shows a comparison between the mean of results of our method against those of the naive method performed on subsets of 1000 randomly chosen users from the test set as described above. From these results, we remark that our method outperforms the naive method for the prediction of trust relations. A standard two tail, paired t-test of these results returns a P-value of 0.0192, showing this difference in results to be statistically significant to the 95% confidence level. Given the potentially suboptimal nature of the parameters used, as mentioned above, the likely discovery of a more optimal set of values for the parameters can only result in a further improvement to these results. Indeed, we can conclude, that the existence of shared items alone is not necessarily a discriminant feature to infer a trust between two users. On the other hand, we remark that the two methods perform very similar rates of prediction of distrust relations, with a slight superiority of our method. This can be explained by two facts; firstly, the fact that the existence of a distrust relation is not explicitly provided by the Epinions dataset. Secondly, due to the shrinking diameter aspect of social networks, the data used will evolve over time and with it, new trust relations will be created. This means that the results of our formula, especially the *FP*, can be improved if we take a more evolved version of the graph.

Table 2: Prediction rate

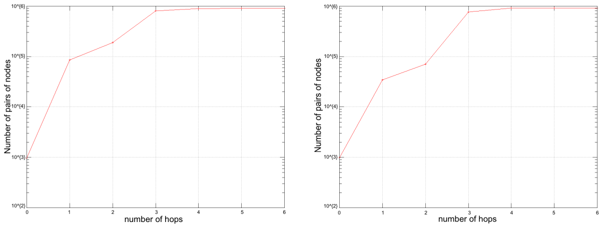
	Trust relation	Distrust relation
Our method	**61.75** %	**73.80** %
Naive method	49.20 %	73.50 %

As a secondary validation of our trust inference formula, we have analyzed the structural properties of the graph computed with our formula, to check its validity to the structural properties typical of social networks. To do this, we compared the properties of the computed graph to those of the real trust graph of the epinions dataset. For this comparison, we have plotted (see Figures 2, 3 and 4), the degree distribution, the hop plo, and the clustering coefficient of both graphs for the same subset of 1000 users, considering only the edges in the computed graph which correspond to a trust assertion according to the threshold. As we can see, all three structural properties are very similar for both the real trust graph and the computed trust graph. From this comparison, we can conclude that our trust inference formula contains the principle properties typical of social networks [2, 16], and thus, as intended, our formula computes a new social trust graph connecting users.



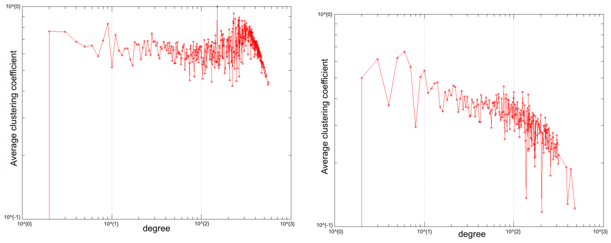
(a) Constructed graph (b) Ground truth graph

Figure 2: Degree Distribution



(a) Constructed graph (b) Ground truth graph

Figure 3: Hop Plot



(a) Constructed graph (b) Ground truth graph

Figure 4: Clustering Coefficient

5. CONCLUSION

In this paper, we investigate the need for the inference of trust from a bipartite social network. Our investigation was inspired by a set of real life observations. Particularly, we remark that the existence of highly rated shared items between two users does not provide good discriminant features for the prediction of trust. Based on these observations, we provide a metric measure that allows the computation of trust between pairs of actors based on their shared items, and a two-hop neighbourhood. Through a set of experiments performed on a real social network, our method shows a high degree of accuracy for the prediction of true trust assertions between users, as well as producing a new computed trust graph connecting all users, which displays all structural properties typical of social networks.

Based only on the topology of a bipartite social graph, the proposed trust measure constitutes a reusable and generic formula. However, our formula still has room for improvement. An interesting direction for future work for the improvement of the method could be the consideration of the content of vertices and edges. In addition to this improvement, we are working on a further validation of our method by integrating it into (1) a trust-based recommendation system and (2) a "*people you may know*" algorithm. In a computation context, our perspective is to provide a high scale implementation of our method on top of large scale graph processing engines, especially, Apache Giraph which is based on the BSP programming paradigm.

6. REFERENCES

[1] G. Adomavicius and A. Tuzhilin. Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions. In *Knowledge and Data Engineering*, volume 17 of *IEEE Transactions*, pages 734–749, 2005.

[2] L. Akoglu and C. Faloutsos. Rtg: A recursive realistic graph generator using random typing. In W. L. Buntine, M. Grobelnik, D. Mladenic, and J. Shawe-Taylor, editors, *ECML/PKDD (1)*, volume 5781 of *LNCS*, pages 13–28. Springer, 2009.

[3] W. Barry. Computer networks as social networks. In *Science*, volume 293, pages 2031–2034, 2001.

[4] S. Brin and L. Page. The anatomy of a large-scale hypertextual web search engine. *Computer Networks*, 30(1-7):107–117, 1998.

[5] T. DuBois, J. Golbeck, J. Kleint, and A. Srinivasan. Improving recommendation accuracy by clustering social networks with trust. In *ACM RecSys'09 Workshop on Recommender Systems & the Social Web*, Oct. 2009.

[6] T. DuBois, J. Golbeck, and A. Srinivasan. Rigorous probabilistic trust-inference with applications to clustering. In *International Joint Conference on Web Intelligence and Intelligent Agent Technology*, WI-IAT'09, pages 655–658, Washington, DC, USA, 2009. IEEE Computer Society.

[7] T. DuBois, J. Golbeck, and A. Srinivasan. Predicting Trust and Distrust in Social Networks. In *2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing*, pages 418–424. IEEE, Oct. 2011.

[8] J. Golbeck. Generating predictive movie recommendations from trust in social networks. In *Trust Management*, volume 3986 of *iTrust'06*, pages 93–104, Berlin, Heidelberg, 2006. Springer Berlin / Heidelberg.

[9] J. Golbeck. Trust and nuanced profile similarity in online social networks. In *ACM Trans. Web*, volume 3, pages 1–33, 2009.

[10] J. A. Golbeck. *Computing and applying trust in web-based social networks*. PhD thesis, University of Maryland, 2005.

[11] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Progation of trust and distrust. In *13th international conference on World Wide Web*, WWW'04, pages 403–412, 2004.

[12] C.-W. Hang and M. P. Singh. Trust-based recommendation based on graph similarity. In *13th AAMAS Workshop on Trust in Agent Societies*, 2010.

[13] P. Jaccard. The Distribution of the Flora in the Alpine Zone. *New Phytologist*, 11(2):37–50, 1912.

[14] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *12th international conference on World Wide Web*, WWW'03, pages 640–651, New York, NY, USA, 2003. ACM.

[15] E. A. Leicht, P. Holme, and M. E. J. Newman. Vertex similarity in networks, Oct. 2005.

[16] J. Leskovec, D. Chakrabarti, J. Kleinberg, C. Faloutsos, and Z. Ghahramani. Kronecker graphs: An approach to modeling networks. *J. Mach. Learn. Res.*, 11:985–1042, Mar. 2010.

[17] J. Leskovec, D. Huttenlocher, and J. Kleinberg. Predicting Positive and Negative Links in Online Social Networks. Mar. 2010.

[18] P. Massa and P. Avesani. Trust Metrics in Recommender Systems. In J. Karat, J. Vanderdonckt, and J. Golbeck, editors, *Computing with Social Trust*, Human-Computer Interaction Series, chapter 10, pages 259–285. Springer London, London, 2009.

[19] P. Massa and B. Bhattacharjee. Using Trust in Recommender Systems: An Experimental Analysis Trust Management. In C. Jensen, S. Poslad, and T. Dimitrakos, editors, *Trust Management*, volume 2995 of *LNCS*, chapter 17, pages 221–235. Springer Berlin / Heidelberg, Berlin, Heidelberg, 2004.

[20] J. O'Donovan. Capturing trust in social web applications. In G. Jennifer, editor, *Computing with Social Trust*, volume 3, pages 213–257, 2009.

[21] L. Page, S. Brin, R. Motwani, and T. Winograd. The pagerank citation ranking: Bringing order to the web. Technical Report 1999-66, Stanford InfoLab, November 1999. Previous number = SIDL-WP-1999-0120.

[22] P. Resnick, N. Iacovou, M. Sushak, P. Bergstrom, and J. Riedl. Grouplens: An open architecture for collaborative filtering of netnews. In *1994 ACM Conference on Computer Supported Collaborative Work Conference*, pages 175–186, Chapel Hill, NC, 10/1994 1994. Association of Computing Machinery, Association of Computing Machinery.

[23] B. Smyth and J. O'Donovan. Trust in recommender systems. In *10th international conference on Intelligent user interfaces*, pages 167–174, 2005.

[24] P. Victor, C. Cornelis, M. D. Cock, and A. Teredesai. Trust- and distrust-based recommendations for controversial reviews. *IEEE Intelligent Systems*, 26(1):48–55, 2011.

[25] F. E. Walter, S. Battiston, and F. Schweitzer. A model of a trust-based recommendation system on a social network. *Autonomous Agents and Multi-Agent Systems*, 16(1):57–74, Feb. 2008.

[26] J. Wang, J. Yin, Y. Liu, and C. Huang. Trust-based collaborative filtering. In *FSKD*, pages 2650–2654. IEEE, 2011.

[27] J. Weng, C. Miao, and A. Goh. Improving collaborative filtering with trust-based metrics. In H. Haddad and H. Haddad, editors, *SAC*, pages 1860–1864, New York, NY, USA, 2006. ACM.

[28] E. Zheleva, L. Getoor, J. Golbeck, and U. Kuter. Using friendship ties and family circles for link prediction. In *2nd ACM SIGKDD Workshop on Social Network Mining and Analysis (SNA-KDD)*, 2008.

[29] C.-N. Ziegler and J. Golbeck. Investigating interactions of trust and interest similarity. *Decision Support Systems*, In Press, Corrected Proof.

[30] C.-N. Ziegler and G. Lausen. Analyzing correlation between trust and user similarity in online communities. In C. Jensen, S. Poslad, and T. Dimitrakos, editors, *Trust Management: Second International Conference, iTrust 2004*, LNCS, pages 251–265. Springer, 2004.