Journal of Computer Science 8 (9): 1496-1500, 2012
ISSN 1549-3636

Current Trust Inference Mechanisms in Web Based Social Networks

Zeinab Dehghan,
Yahya AlMurtadha, Lai Ngan Kuen and Zailan Abdul Salam
Department of Software Engineering,
Faculty of Computer Science and Information Technology,
Asia Pacific University, College of Technology and Innovation,
Technology Park Malaysia Bukit Jalil, 57000 Federal Territory of Kuala Lumpur, Malaysia

Abstract: Problem statement: Nowadays, web based social networks have gained a lot of attention. Over one billion users participate, communicate and share information on these networks based on trust. **Approach:** One important issue on online social networks is how much one person can trust another person in the network whom they are not directly connected. Scholars around the world have introduced a variety of models and algorithms for inferring trust in online social networks. This study takes a deep look at current methods, their advantages and disadvantages. **Results:** All current methods have weaknesses and cannot be considered the best solution for inferring trust. **Conclusion:** Considering the fact that web based social networks are based on trust upon participants, a more accurate and fast algorithm is needed to infer trustworthiness and help users gain valuable information.

Key words: Algorithm, trust value, social network analysis

INTRODUCTION

Due to the rapid growth in computer networking technologies, Web Based Social Networking (WBSN) is significantly gaining popularity. Human computer interaction has definetly chnged old communication styles. Anyhow, social network applications yet cannot acquire wider acceptance by many people because of issues such as privacy, trust and security (Aboud, 2007). In WBSNs users tend to share information based on trust levels (Adali *et al*., 2010). For solving trust issues caused by malicious users in the social networks, trust calculation models were proposed (Jiang *et al*., 2011).

Upon appearance of semantic web, many applications and systems require static trust mechanisms. Semantic web is extension of the current web that contents are comprehensive so machines and computers could be able to understand. Considering the fact that more intelligent agents will take place of human tasks every day, they will need an automated method for inferring trust so trust inference mechanism has become a critical issue (Victor *et al*., 2011).

The issue of trust is illustrated in Fig. 1. In the social network, trust studies whether a user (*trustee*) behaves as expected by an interested user (*trustor*) through a number of other users (*recommenders*). From this network the trust graph is simulated which consists of trustees, trustors, recommenders and their relationships. Any online social network can be presented as graph *G*, where any individual profile is a node and the relationship between 2 nodes is the edge of the graph (Nagle and Singh, 2009).

Peter? John dose not now Peter, But John knows Tom and Ben whom both know Peter.

Web based social networks can be modeled as graphs. This is done in order to analyze and study behaviors of the network (Gaol and Widjaja, 2008) A sample of a social network graph is illustrated in Fig. 2.

Trust inference algorithms are used to calculate the trust value between two nodes of the trust graph which are not directly connected. The main reason of using mathematical and graphical methods in the analysis of social network is to present and describe the networks systematically and compactly.

Major researches have been conducted worldwide to find suitable algorithms for inferring the optimal path and the trust value. The presented literature review is a brief look at various trust inference mechanisms presented by scholars in recent years. The mechanism, implementation on data sets, results, benefits and weaknesses of each method is discussed.

Current trust inference mechanisms: There are several trust inference mechanisms introduced by scholars worldwide. Below is the list of most recent of these works:

Corresponding Author: Zeinab Dehghan, Department of Software Engineering, Faculty of Computer Science and Information Technology, Asia Pacific University, College of Technology and Innovation, Technology Park Malaysia Bukit Jalil, 57000 Federal Territory of Kuala Lumpur, Malaysia

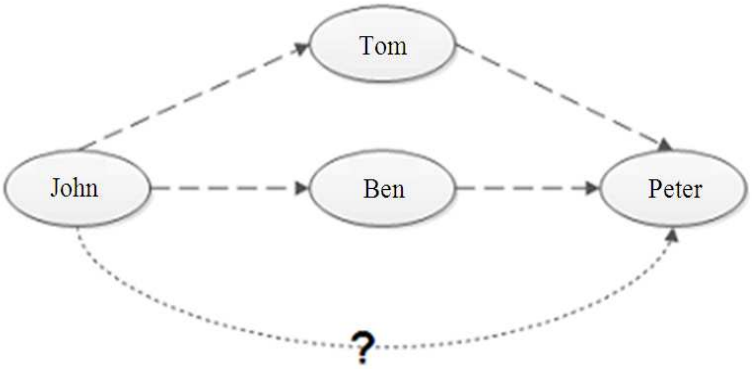

Fig. 1: The issue of trust: John and Peter are not directly connected in the network. How much can John Trust Peter? John dose not now Peter, But John knows Tom and Ben whom both know Peter

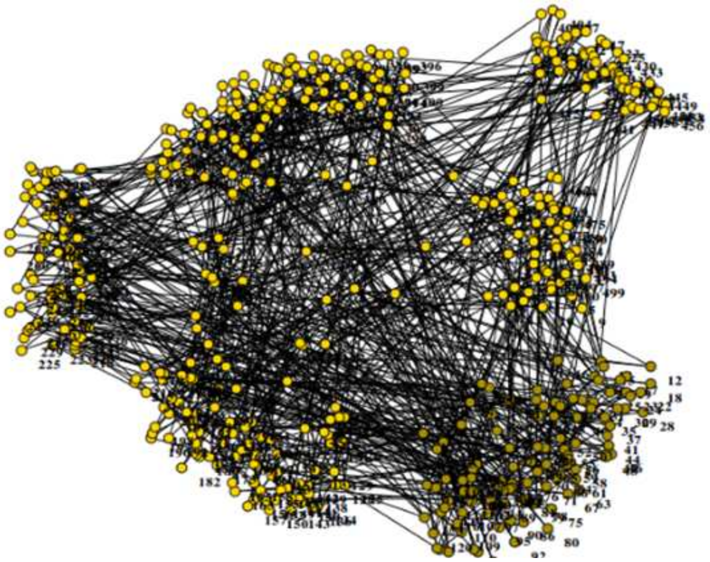

Fig. 2: Sample of a social network graph generated via NodeXL

SocialTrust: *Social Trust algorithm* (Caverlee *et al*., 2008) is a framework based on reputation for trust aggregation. The algorithm used a feedback rating method which involved updating trust value using dynamic revision of trust rating according to three elements: history of rating, current user rating and adaption to change. Caverlee tested this technique in MySpace using five million nodes (users) and nineteen million edges (relationships). The result showed success in identifying malicious nodes. However the weakness of this method is ignoring useful information via eliminating some paths.

RN-trust: *RN-Trust* algorithm (Taherian *et al*., 2008) was brought up in 2008. The main idea for this method is using Resistive Network (RN) concept to simulate trust networks. All relationships between 2 people are modeled via resistor in the way that more trust value means lower value for corresponding resistor. In this was trust network is transformed to Resistive Networks (RN). This model used trust values in the continuous range of [0, 1]. This algorithm was applied in the same sample network as Tidal Trust and proved to give better results. A major problem of this method is the time complexity of the algorithm which is polynomial (O (v^3) v= number of nodes in the network graph).

Bayesian: *Bayesian* trust inference mechanism for very complex WBSN was suggested in 2009 (Liu *et al*., 2009; 2010). Liu introduced a compound trust oriented

WBSN structure that included very complex social relationships. The main improvement of this method was delivering realistic trust values between the "trustee" and "truster" via considering logic "AND" between paths. Although experiments resulted in success, the initial principles defined for extracting trust are actually not used in major WBSNs.

Combined trust model: *Combined Trust Model* (Yu and Wang, 2010) was a model which described how to infer the trust value in combine with network topology and the usage of web mining. The method involved three main phases: Building an individual trust network in order to determine transitive path for the destination user, calculating the social influence value for middle nodes and finally exploring interaction frequency of the user to filter the trust measurement. This research used TWT online community data and SNS website data to test efficiency of the proposed model. The main advantage of this method is using "middle node" which helps obtaining a more accurate trust value. Beside benefits of this method, there is a major problem. The data set which is used for testing the method is a small data set so there is a probability that in large networks, the results may not be optimum.

Matrix factorization: *Matrix Factorization* (Jamali and Ester, 2010) technique was introduced in 2010. This model has used the social influence of the behaviour of all neighbours of a node. This influence is formulated and considered. This method has been tested using both Epinions.com and Flixster.com Data sets. Comparing the results with previous techniques showed clear outperformance. An important gap of this method is the fact that it cannot handle negative trust values, but in real world, some social networks allow users to give negative values as a way to show distrust.

H_OSTP: H_OSTP a *Heuristic algorithm* for inferring trust (Liu *et al*., 2009; 2010) was introduced in 2010 which focused on finding the optimum path between nodes in the social network. A new concept "Quality Of Trust (QOT)" was added in this method. The participants of this network were recommendation, social relationship, trust information and quality of trust. Unlike previous techniques, this method is suitable for very large scale networks. It has been tested on "Enron Email" which is very large public data set. The experiment proved the algorithm to have a lower time complexity and optimum path selection in comparison to previous work. A major weakness of this method is the necessity of aggregating values for every QOT feature in each social network trust path that connects the source node and the sink.

FlowTrust: *FlowTrust* algorithm (Wang and Wu, 2011) supports multi-dimensional trust. Confidence level and trust value were two factors considered in this method. This algorithm uses a flow trust approach to model any trust graph containing network flow. Then by using the flow theory, maximum value of trust that is able to flow amongst the graph is evaluated. Comparing this mechanism with previous ones resulted in better normalized trust values. However the main weakness still remains; flowTrust is capable of handling small trust graphs due to the fact that the algorithm is not efficient in very large networks. Since current web based social networks are huge, containing tons of data, it is not likely to produce a small trust graph out of the large network.

Trust and distrust prediction: A model for predicting Trust and distrust in WBSN was introduced by DuBois *et al*. (2011). This model is a combination of customized spring embedding method and trust inference algorithm rooted on the random graph theory. The method has been tested on three data sets of Epinions, Wikipedia election and Slashdot in order to review efficiency. Results showed that the algorithm is capable of suitably organizing concealed edges in the social network graph as "good" or "bad" edges with a high precision. A major advantage of this algorithm in comparison to the previous ones is the fact that it calculates the distrust as well as trust. This is very useful for deriving negative edges in the network graph so they can be left out of the search path. This method also has the capability of finding "positive" edges so they can be considered in the search past for gaining best result of trust value. Despite advantages of this method, it has a number of weaknesses. Firstly, online social networks often do not have a distrust value so only a few websites can use this method. Secondly the method is designed for undirected graphs so the network graph is treated as undirected and this approach affects the results leaving out information. Finally in the case where there are a lot of nodes connected with distrust value, this method is Inefficient.

MATERIALS AND METHODS

Introduced models for inferring trust value in WBSN use different methods. *Social Trust* utilizes a feedback rating method and updates the trust value frequently. *RN Trust* makes use of resistive networks to model the WBSN and calculate the trust value between participants of the network. The method applied by *Bayesian* is placing logic "AND" among paths of the network graph. *Combined Trust Model* uses "network topology" in combination with "web mining" as a method to infer trust in online social networks. The method considered by *Matrix Factorization* is formulating the behavior of neighbor nodes and calculating trust value regarding to this formula. *H_OSTP* utilizes the concept of QOT (quality of trust) and finds optimum path between two nodes in the network graph. *Flow Trust* produces a normalized trust value via applying the "flow theory". Trust and distrust prediction employs a combination of customized spring embedding method and trust inference algorithm rooted on the random graph theory in order to infer the trust value.

RESULTS

Each model described in previous sections has been applied in real WBSNs in order to view efficiency and further analyzing. Table 1 shows the results of applying all mentioned methods using standard data sets of real social networks.

DISCUSSION

Most recent methods for inferring trust in WBSNs have been analyzed. Each model has its own strengths and weaknesses which should be considered when applying to real online social networks. It is better to be said that each method is useful for a particular type of network. Some networks are large scaled and prefer to use a more simple method with lower time complexity. In some other business related WBSNs, it is necessary to make an accurate trust value no matter what time it takes to produce the result. Choosing an appropriate method totally depends on the characteristics of the network.

Table 1: Methods and results

Method	Result
Social Trust	This technique was tested on MySpace using five million nodes (users) and nineteen million edges (relationships). The result showed success in identifying malicious nodes.
RN-Trust	This technique was compared to tidaltrust and proved to make better results but in the time complexity of $O(v^3)$
Bayesian	Applying logic resulted in a more realistic trust value compared to other techniques.
Combined Trust	Resulted in accurate trust value when applied to TWT online community data and SNS website, however is only suitable for small scale WBSNs.
Matrix Factorization	Tested on Epinions.com and Flixster.com Data sets resulted in clear outperformance but yet cannot handle negative trust values
H_OSTP	Resulted in lower time complexity and optimum path selection when tested on Enron email data.
FlowTrust	Appling the method resulted in better normalized trust values although it is only capable of handling small data sets.
Trust and distrust prediction	Results showed that the algorithm is capable of suitably organizing concealed edges in the social network graph as "good" or "bad" edges with a high precision.

CONCLUSION

Current trust inference methods rely on simple trusts networks where only trust between neighbor nodes is considered. Current trust inference mechanisms are not producing realistic results. Many social factors and psychology issues that influence the trust value are not considered by proposed methods. Many of these techniques lack appropriate definition of trust and its perspectives. Major of the introduced algorithms have a high time complexity which makes them useless in real world. More research is necessary in this area in order to produce a more valuable algorithm with lower time complexity and higher accuracy which does consider the social aspects of trust in real word.

REFERENCES

Aboud, S.J., 2007. Efficient Anonymous and Non-Repudiation E-Payment Protocol. Inform. Technol. Advisor.

Adali, S., R. Escriva, M.K. Goldberg, M. Hayvanovych and M. Magdon-Ismail, 2010. Measuring behavioral trust in social networks. Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI), May, 23-26. IEEE Xplore Press, Vancouver, BC, Canada, pp: 150-152. DOI: 10.1109/ISI.2010.5484757

Caverlee, J., L. Liu and S. Webb, 2008. Towards robust trust establishment in web-based social networks with socialtrust. Proceedings of the 17th International Conference on World Wide Web, Apr. 21-25, ACM Press, Beijing, China, pp: 1163-1164. DOI: 10.1145/1367497.1367707

DuBois, T., Golbeck, J. and A. Srinivasan, 2011. Predicting trust and distrust in social networks. Proceedings of the IEEE 3rd International Conference on Social Computing (socialcom) Privacy, Security, Risk and Trust (passat), Oct. 9-11, IEEE Xplore Press, Boston, MA, pp: 418-424. DOI: 10.1109/PASSAT/SocialCom.2011.56

Gaol, F.L. and B. Widjaja, 2008. Framework of regression-based graph matrix analysis approach in multi-relational social network problem. J. Math. Stat., 4: 51-57. DOI: 10.3844/jmssp.2008.51.57

Jamali, M. and M. Ester, 2010. A matrix factorization technique with trust propagation for recommendation in social networks. Proceedings of the 4th ACM Conference on Recommender Systems, Sep. 26-30, ACM Press, Barcelona, Spain, pp: 135-142. DOI: 10.1145/1864708.1864736

Jiang, J., J. Xiang, H. Zhou, X. Zheng and T. Dong, 2011. Trust Calculation Model Based on Social Network and Evidence Theory. Proceedings of the IEEE International Joint Conference on Service Sciences (IJCSS), May, 25-27, IEEE Xplore Press, Taipei, pp: 173-177. DOI: 10.1109/IJCSS.2011.41

Liu, G., Y. Wang and M. Orgun, 2009. Trust inference in complex trust-oriented social networks. Proceedings of the International Conference on Computational Science and Engineering, Aug. 29-31, IEEE Xplore Press, Vancouver, BC, pp: 996-1001. DOI: 10.1109/CSE.2009.248

Liu, G., Y. Wang, M.A. Orgun and E.P. Lim, 2010. A heuristic algorithm for trust-oriented service provider selection in complex social networks. Proceedings of the IEEE International Conference on Services Computing, July, 5-10. IEEE Xplore Press, Miami, FL, pp: 130-137. DOI: 10.1109/SCC.2010.47

Nagle, F. and L. Singh, 2009. Can friends be trusted? Exploring privacy in online social networks. Proceeding of IEEE International Conference on Advances in Social Network Analysis and Mining, July, 20-22, IEEE Xplore Press, Athens, pp: 312-315. DOI: 10.1109/ASONAM.2009.61

Taherian, M., M. Amini and R. Jalili, 2008. Trust inference in web-based social networks using resistive networks. Proceedings of the 3rd International Conference on Internet and Web Applications and Services, Jun. 8-13, IEEE Xplore Press, Athens, pp: 233-238. DOI: 10.1109/ICIW.2008.41

Victor, P., C. Cornelis and M.D. Cock, 2011. Trust Networks for Recommender Systems. 1st Edn., Atlantis Press, ISBN: 10-9491216074, pp: 216.

Wang, G. and J. Wu, 2011. FlowTrust: Trust inference with network flows. J. Frontiers Comput. Sci. China, 5: 181-194. DOI: 10.1007/s11704-011-0323-4

Yu, X. and Z. Wang, 2010. A enhanced trust model based on social network and online behavior analysis for recommendation. Proceedings of the International Conference on Computational Intelligence and Software Engineering (CISE), Dec. 10-12, IEEE Xplore Press, Wuhan, pp: 1-4. DOI: 10.1109/CISE.2010.5676798