A Survey of Web-based Social Network Trust

Eric Wang
Department of Computing
Macquarie University
Sydney, Australia
eric.wang1@students.mq.edu.au

Abstract

Trust computing has become more important on Web-based Social Networks (WBSNs), such as MySpace, Facebook, and LinkedIn where people interact and seek information based on trust. On existing WBSN platforms, users can explicitly specify trust value to which they have direct relationship with. The user can then make a decision based on this trust value of others and their opinions. However, the user may seek information from others who are not directly connected to him. Then the user needs to determine whether the reliability of information and ensure it is not from a malicious user who gives false information. The aim of this paper is to present an overview of existing trust inference mechanisms that are designed on solving this problem. Analysis and comparison are made to identify issues for future studies.

1 Introduction

On a Web-based Social Network (WBSN), such as Facebook, MySpace, LinkedIn, and LiveJournal, information is created and consumed by its users. Users share information based on the level of trust they explicitly assign to other users. The ability to determine how much a user trusts the source of the information when the user does not know the source directly can be used for aggregating, filtering, and ordering of information. Additionally, if trust can be estimated accurately, the user can then use this trust estimation to make decisions on the information.

For trust estimation to be useful on WBSN, it is often expressed as trust ratings or values that a user can explicitly assign to another user. We can then use those trust values to infer the trust that may exist between two people who are not directly connected. In another word, when trust is explicitly rated on a numerical scale, this network data can be composed to produce information about the trust between two individuals without a direct connection. [Jennifer Golbeck, James Hendler, Nov 2006].

Trust inference estimation must be simulated into an efficient and accurate mathematical algorithm, or mechanism, to calculate the trust inference value. The structure of the social network and explicit trust value between two directly connected users can be used in this calculation. Further more, this mechanism needs to be effective against malice attacks from users who give false trust values to benefit themselves.

This trust inference value can enable users to make reasonable decision on the basis of the trust relationship in the WBSN with certainty and degree of confidence.

The rest of the paper is organised as follows; in section 2, we discuss what trust is and what trust inference is in the context of WBSN. In section 3, analysis and comparisons are performed on a collection of mechanisms designed for determining trust inference value. Then in section 4, we discuss the finding and outcome of this paper. Lastly in section 5 we conclude this paper by presenting some issues for future studies.

2 Trust Definition and Characteristics

The verb trust, general terms, can mean to have belief or confidence in the honesty, goodness, skill or safety of a person, organization or thing [Cambridge Dictionaries Online, 2009], or simply to have confidence or faith in [Jennifer Golbeck., 2005].

Some social network sites have trust implied in their network structure. For instance, “LinkedIn connects you to your trusted contacts and helps you exchange knowledge, ideas, and opportunities with a broader network of professionals” [learn.linkedin.com/what-is-linkedin/].

In this paper, we define trust in the context of WBSN, as where a person believes the action he/she makes will be a desirable result if the per-

son is to rely on the belief of another person or persons.

To simulate trust in the WBSN environment, J. Golbeck and J. Hendler [Jennifer Golbeck, James Hendler, Nov 2006], propose that there are three main properties of trust. They are transitivity, asymmetry, and personalisation.

They propose that trust is not perfectly transitive in the mathematical sense where if Alice trusts Bob, and Bob trusts Charles, then it is not necessarily true for Alice to trust Charles in the same level of trust. Also, there are two aspects of transitivity of trust, where there is the trust in a person, and then there is the trust in the person's recommendations of other people. For example, Alice may trust Bob's opinion on music, but not trust him on recommending on other people on their opinions about music.

The second property, trust asymmetry, means trust is not necessarily the same in both directions between two users. For example, Alice trusts his supervisor Bob, but Bob may not trust Alice with the same amount of trust.

The third property is trust personalisation, where it is suggested that inherently trust is a personal opinion. Alice and Bob may have very different opinion about Charles; however, there is no absolute correct or incorrect value except from the perspective of Alice and Bob. This is in contrast to a reputation system such as in a P2P network where there is a global value of trust on a particular node or user.

In Figure 1, we demonstrate what trust inference is. We can say A, or the "source", is directly connected with B and C, but is not directed connected to D, E, F, or G. Further more, we can say A is indirectly connected to G via four paths, A->B->D->E->G, A->C->D->F->G, A->B->D->F->G, and A->C->D->E->G, thus creating four perspectives or trust inference values of G, or the "sink", when we are determining the trust inference value of A to G.

A trust inference mechanism can be decribed as an algorithm which determines the inference trust values which are recommendations to one user about how much to trust another user. This algorithm can generate a recommended trust rating for an unknown person in the social network, based on information from others user connecting to this unknown user.

Modeling a trust inference mechanism is achieved by assigning the persons in a WBSN as nodes and friendships or relationships as directed edges, while trust values as edge labels.

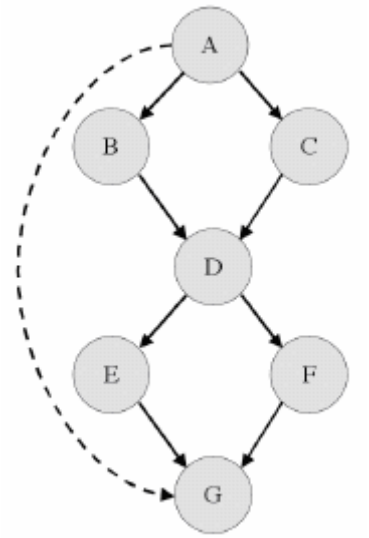

Fig 1: Trust Inference from node A to node G

3 Trust Inference Mechanisms

There are many trust inference mechanisms propose by scholars around the world, showing the popularity of this topic. However, at the same time, this indicates the topic is yet to mature into industry standards from various existing mechanisms.

The following subsections are a collection of trust inference mechanisms designed for WBSNs. Some are algorithms; others are models that can be more complex.

All of the trust inference mechanisms test their accuracy by taking an existing social network data set, and then arbitrarily take away selective number of direct links. Then trust inference calculation is performed on those links, and finally the result of their trust inference value and the explicit trust value of the direct links are compared to determine the accuracy of the trust inference mechanism.

3.1 TidalTrust

The TidalTrust algorithm is proposed by Golbeck [2005]. It considers the trust values to be numbers in a continuous range of [0..10]. It is simple and its low complexity (O(V + E)) allows high scalability in its application.

Golbeck assumes trust values inferred through shorter paths may be more accurate, thus only the shortest paths from source to sink are considered. This works for the algorithm because it simplified the algorithm; however, its weakness is it excluded information that may be useful from nodes of longer paths, especially the case where majority of the nodes in the longer path may have more trusted nodes.

TidalTrust algorithm is known as a famous and highly cited algorithm for inferring trust. Many other algorithms found in this paper make comparison of their trust algorithm with TidalTrust.

3.2 Binary Trust Algorithms and TrustMail

Two algorithms propose by Jennifer Golbeck, James Hendler [Nov 2006] aim to develop efficient and accurate mechanisms for inferring trust relationships that use only the structure and trust ratings within a social network. They integrate them based on binary trust assignment (zero or one) and input the results into an experimental email client application called TrustMail to enhance email filtering.

The Binary Trust algorithms are the Rounding Algorithm and the Non-Rounding Algorithm. Both of which use binary value (0 for not trustworthy while 1 is trustworthy) to explicitly indicate trust value assign at each node. Both give similar results but Rounding Algorithm is more accurate than non-rounding at each node of the calculation, when over half of the nodes are "good nodes" that provide true trust values most of the time. This is because rounding at each node removes more error than only performing the rounding at the last node.

Both algorithms calculate a result based on the percentage of each node's adjacent nodes that rates the node as good (value of 1) or bad (value of 0). Their experimental results show increase in bad nodes does not significantly reduce the accuracy of the results. Thus both algorithms are robust against malicious attacks from users, or "bad nodes" which intentionally provide false trust values.

Their experimental email client software, TrustMail, can replace the manual process of verifying the trustworthiness of the information about an email sender/recipient by utilising the data in WBSN, thus assists in filtering emails and can work in conjunction with spam filtering software. This works by the user rates an email recipient that the user knows directly, and each email received in the inbox will be rated by a trust inference value calculated by their binary trust algorithm. This is to achieve higher ratings to non-spam senders.

The researchers admit that this filtering method does not replace the currently used agent based approach such as blacklisting and white listing email filtering, but can act a complementary system to ease email overload on users.

3.3 Advogato Trust Metric

This trust mechanism propose by Raph Levien [2002] calculates trust by using a network flow model. It issues 3 levels of certification between users to determine the user trust value within a group.

Advogato uses the same trusted nodes to make trust calculation for all users, thus it is a global trust algorithm suitable for P2P. However, a common modification is to set the user as the trusted node, therefore transforming it to a local trust algorithm suitable for WBSN.

Advogato calculates trust inference by identifying individual bad nodes and finding any nodes that certify the bad nodes, the metric eliminates the unreliable section of the network, making it more resistant to malicious users.

The underlying code for this trust inference mechanism has been released under a free software license. Because of this, it has been the basis of numerous research papers on trust metrics and social networking including some researchers who argue that this metric can be attacked in certain scenario [Jesse Ruderman, 2004].

3.4 Appleseed

Appleseed, develop by Cai-Nicolas Ziegler, Georg Lausen [2004], is a group trust metric that uses spreading activation strategies. It is based on finding the principal eigenvector and covers many conditions.

This mechanism is also attack resistant but requires performing normalisation on trust values. A weakness in this algorithm is that in calculating the normalised trust value, it means a person who has made many high trust ratings will have lower value than if only one or two people had been rated. It is possible to have very high trust for a large number of people and that trust should not be any weaker than the trust held by a person who only trusts smaller number of people.

Another weakness of this mechanism is that it requires exponentially higher computation with increasing number of users, thus not scalable due to this complexity.

3.5 SocialTrust

SocialTrust, propose by James Caverlee, et al [2008], is a reputation-based trust aggregation framework for supporting tamper-resilient trust establishment in WBSNs.

Two main features of this mechanism are its dynamic revision of trust by differentiates relationship quality from trust, and it includes a per-

sonalised user feedback mechanism to adapt to the social network as it evolves.

SocialTrust updates trust value through dynamic revision of trust ratings according to the following three components: the current rating, the history, and the adaptation to change.

This mechanism is relatively new and has been tested on MySpace with over 5 million nodes and over 19 million relationship links. Its initial experiment results show that SocialTrust is more robust against malicious users where its trust inference value accuracy remains relatively unchanged as percentage of malicious users increases due to its link quality and feedback ratings mechanism.

3.6 FuzzyTrust Algorithm

Mohsen Lesani and Saeed Bagheri [2006] consider the problem where trust inference in a large social network can encounter contradictory information. They propose fuzzy linguistic terms to specify trust to other users and developed an algorithm based on these.

This algorithm computes trust from stronger and shorter paths as it performs a breadth-first-like search through the nodes to find shortest paths and also to find the path from source to sink strength fuzzy set.

It is able to handle conflicting trust values by using fuzzy linguistic expression (e.g. low, medium, high), which is easier for users to assign trust.

It is simulated and compared with another algorithm, TidalTrust by Golbeck, but the results of Lesani's simulation indicate that the fuzzy algorithm offers more precise information than the TidalTrust. However, because of that he uses TidalTrust algorithm as the basis of his fuzzy algorithm, it has the same drawbacks of TidaTrust algorithm.

3.7 SUNNY

Ugur Kuter and Jennifer Golbeck [2007] develop a trust inference algorithm that uses a probabilistic sampling technique to estimate a user's confidence in the trust information from designated sources. It computes an estimate of trust based on only those information sources with high confidence estimates, regardless path length, to achieve higher accuracy trust estimates. This is in contrast to TidalTrust where only shortest paths are considered.

It differs to other algorithm in that it claims to be the first trust inference algorithm which includes a confidence measure in its computation. It is more accurate against Golbeck's own TidalTrust when tested with data from FilmTrust social network.

3.8 Trusted Gossip

The two researchers, Arindam Mitra and Mucumaru Maheswaran [2007], propose a trusted gossip protocol for disseminating popular information from reputable users while restricting flow of spam messages. This is so that good information can still be spread effectively by word of months while reduces the negative effect of unwanted information that we call spam.

The algorithm estimates trust via a Bayesian trust estimation process where information are tagged and processed, then the trust value is evaluated through a recommender system.

They present three approaches for this recommender system. Receiver Initiated, Sender Initiated, or using both as Hybrid, where node-level filtering and message-level filtering are implemented at the sender and/or the receiver side.

Their research uses a subset of Flickr social network users and find this subset of randomly selected users can reach most other users within 6 hops, but no path is found between many users, where inference trust can not be evaluated. They also find 3 hops is the limit for likeminded nodes where trust evaluation is more accurate.

Their main findings are that message level filtering done at the originating nodes is the more accurate method of determining inferred trust. They also prove by experimenting on other WBSNs that this Trusted Gossip mechanism is robust against reputation distribution.

3.9 RN-Trust

In this algorithm, Mohsen Taherian et al propose using a resistive network concept, similar to the idea of electrical resistance, to simulate trust networks where a resistive network is a collection of resistors that represent trust value as reverse of the resistance.

In this algorithm, the trust network is mapped to a resistive network, and a voltage source connects from u to v, while the electrical current flows between u and v. This current can be interpreted as the trust relation from u to v. If there is a resistor between u and v, then the amount of current flows from u to v decreases. Thus, the higher the trust value, the lower the value of the resistor.

Similar to how TidalTrust assigns trust values, the trust values in this algorithm are continuous values in the range of [0, 1].

This trust inference algorithm resolves many problems of the previous ones. For instance, it does not need to ignore trust inference derive from long path by consider the full length of the trust inference path, rather than only the shortest ones, giving a more complete overview in determining the inference trust value. This addresses the major weakness in the TidalTrust algorithm where some information along the path which may affect the accuracy of the calculation is ignored. In addition, the algorithm is very simple and its time complexity is polynomial, thus highly scalable.

4 Findings and Outcome

4.1 Approach of the Problem

Scholars approach the problem of developing a trust inference mechanism from different perspectives. Firstly, algorithms such as TidalTrust, Binary Trust, and FuzzyTrust make the assumption that only trust values in the shortest or strongest paths are included in their calculation to achieve simplicity with sufficient accuracy. Secondly, Advogato uses a network flow model to control how trust is inferred. Thirdly, mechanism can perform more than one step of calculation, e.g. perform a Bayesian trust estimation process, then perform a recommender system, to achieve higher accuracy and improve robustness against reputation distribution as shown in the Trusted Gossip algorithm. Fourthly, SUNNY includes the confidence factor and RN-Trust uses an electrical resistance model to eliminate the weakness in TidalTrust where only trust values in the shortest paths are considered, lastly, there are algorithms which attempt to solve different aspect of trust scenarios. For instance, FuzzyTrust attempts to resolve contradictory information by using fuzzy linguistic terms instead of numeric trust values.

4.2 Merits and Weaknesses

All trust inference mechanisms are more accurate in calculating trust inference values than taking simple average along the path of the trust inference. Mechanism such as Trusted Gossip shows they are robust against variation in trust value distribution and other mechanisms such as Binary Trust algorithms are relatively unaffected by malicious attacks while maintaining simplicity in the algorithms. However, none has comprehensive tests and they were not fully independently tested by another research organisation or commercial entity. This is an indication that the topic is still relatively new and the implementation of those mechanisms in software applications has not been widely spread.

Complexities of some mechanisms such as in the Appleseed and Trusted Gossip algorithms show they may have scalability issues. WBSN that has over millions of members may prove prohibitive for these mechanisms. This is why some mechanisms aim to have efficiency as one of their objectives such as the RN-Trust.

Relationships and trust are dynamic. New relationships are formed everyday and old ones weaken gradually. Some mechanisms take this into account and include in its mechanism a method of updating its trust rating as illustrated in SocialTrust.

4.3 Other Consideration

We also find that PageRank, a rating mechanism used by Google search engine where high ranking is achieved if the sum of the ranks of its back links is high, can be used to compare the effectiveness of a trust inference mechanism. However, having the content as popular does not necessarily indicate its accuracy or authenticity.

5 Conclusion and Future Work

In this paper, we define what trust inference is in a WBSN. We then review a selection of research papers to examine existing trust mechanisms, their properties, and their approach to trust inference calculation.

We discuss some merits and weaknesses in those trust inference mechanisms, considering factors such as accuracy, scalability, robust against reputation distribution, resilience against low confidence level, and attack resistance from malicious users.

From the result of this paper, we can surmise that the maturity of a generally accepted trust inference mechanism is yet to be realised.

Further more; we propose 5 possible future research works which are either in area that is yet to be explored by existing mechanisms, or in area which existing mechanisms can improve.

- Further Improve accuracy and the precision of trust inference value calculation
- Develop an event based trust inference algorithm where only past events are used in the calculation so that it is context focus and can continuously update its trust inference value
- Develop context aware extensions so that the WBSN may support multiple trust

views of each user depending on the context or topic of discussion to improve accuracy and relevance of the trust inference

- Pushing the boundaries of how trust inferences can be applied in WBSN more than a simple email filtering system as applied in TrustMail using Binary Trust. Suggested application in Artificial Intelligence; in particularly, the use in military intelligence gathering where a government needs to determine the trustworthiness of intelligence reports from its agents
- Studies on the requirement of computing resources such as CPU processing power, memory usage, storage requirement, and network traffic generated, when a trust inferring mechanism is applied in a WBSN

Another research topic would be finding a grand unified trust inference mechanism that can adjust its algorithm and logics depending on the topic to provide the most consistently accurate trust inference value estimation. Additionally, this mechanism needs be applicable to not only in WBSN, but also in P2P networks.

References

Arindam Mitra, Muthucumaru Maheswaran, [2007] *Trusted Gossip:A Rumor Resistant Dissemination Mechanism for Peer-to-Peer Information Sharing.* Advanced Information Networking and Applications, 2007. AINA '07. 21st International Conference on. Dept. of Comput. Sci., Manitoba Univ., Winnipeg, MB.

Cai-Nicolas Ziegler, Georg Lausen [2004] *Spreading Activation Models for Trust Propagation.* Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04)

Cambridge Dictionaries Online [2009] *Definition Trust,* viewed on 22 Mar 2009. http://dictionary.cambridge.org/define.asp?key=85211&dict=CALD

James Caverlee, Ling Liu, Steve Webb [2008], *Towards Robust Trust Establishment in Web-Based Social Networks with SocialTrust.* Proceeding of the 17th international conference on World Wide Web. Beijing, China

Jennifer Golbeck., [2005] *Computing and Applying Trust in Web-based Social Networks,* Doctor of Philosophy Dissertation, University of Maryland, College Park.

Jennifer Golbeck, James Hendler [Nov 2006] *Inferring Binary Trust Relationships in Web-Based Social Networks.* ACM Transactions on Internet Technology, Volume 6, Issue 4, New York, NY, USA.

Jesse Ruderman [2004] *A comparison of two trust metrics*. UCSD CSE

Mohsen Lesani and Saeed Bagheri [2006] *Fuzzy Trust Inference in Trust Graphs and its Application in Semantic Web Social Networks.* World Automation Congress, 2006. WAC '06. Sharif University of Technology, Iran.

Mohsen Taherian, Morteza Amini, Rasool Jalili, [2008] *Trust Inference in Web-Based Social Networks Using Resistive Networks.* Internet and Web Applications and Services, 2008. ICIW '08. Third International Conference on 8-13 June 2008. Page(s): 233-238.

Piotr Sztompka [1999] *Trust: A Sociological Theory.* Cambridge University Press, Cambridge, UK.

R. Guha, Ravl Kumar, Prabhakar Raghavan, Andrew Tomkins [2004] *Propagation of Trust and Distrust.* Proceedings of the 13th international conference on World Wide Web, New York, NY, USA

Raphael L. Levien [2002] *Attack resistant trust metrics. PhD thesis,* Department of Computer Science, University of California, Berkeley.

Stephen Paul Marsh [Apr 1994] *Formalising trust as a computational concept.* PhD thesis, Department of Mathematics and Computer Science, University of Stirling.

Ugur Kuter and Jennifer Golbeck [2007]. *SUNNY: A New Algorithm for Trust Inference in Social Networks, using Probabilistic Confidence Models.* Proceedings of the Twenty-Second National Conference on Artificial Intelligence (AAAI-07). Vancouver, British Columbia, July, 2007.

Webster's Online Dictionary [2009] *Definition: Trust*, viewed on 22 Mar 2009. http://www.websters-online-dictionary.org/definition/trust

Young Ae Kim, Minh-Tam Le, Hady W Lauw, Ee-Peng Lim, Haifeng Liu, Jaideep Srivastava,. [Apr 2008] *Building a web of trust without explicit trust ratings* .Data Engineering Workshop, 2008. ICDEW 2008. IEEE 24th International Conference. Page(s): 531-536.