2015 International Symposium on Nonlinear Theory and its Applications
NOLTA2015, Kowloon, Hong Kong, China, December 1-4, 2015

Activity and Content-Based Trust Estimation in Online Social Networks

Trung Son Doan(✉), Mario Kubek and Herwig Unger

Chair of Communication Networks, University of Hagen, Germany
{son.doantrung, dr.mario.kubek, herwig.unger}@gmail.com

Abstract—Online Social Networks provide many possibilities to people to make new contacts all over the world. Nevertheless, the derived friendship relations are usually less confident compared to the real-life friendships due to missing possibilities to built up trust. Therefore, a method is introduced to derive trust from user activities in the network. A global trust judgement is processed considering the mutual influences of all network users and stochastically being confirmed by randomly chosen groups of users. Simulation results show the power of the approach.

1. Introduction

The introduction of online, social networks (ONS) have been welcomed by broad groups of the society which have figured out opportunities of such systems for their activities.

Three scenarios of the use of such systems may be distinguished. People,

1. ... use the OSN, who know each other well from real life and have already established any kind of mutual connection. They use an OSN only as another, fast and world-wide available tool to intensify their communication and share interesting information.

2. ... meet anyhow in the OSN for the first time; usually OSN offer a plenty of methods for doing so for any purpose. They never knew each other before in the real life and share only information on the OSN, which become a complete documentation of this relation.

3. ... knowing each other following the procedure described in 1) or 2) and exchange information on third parties, which are not known to everybody; e.g. a service s is recommended by a group of persons $x_1, x_2, .., x_r$ to another person y.

In the first case, users may refer to some real-life background and therefore a well-established feeling of trust, confidence and friendship, usually derived from the limbic system of the human brain. Public and private key may be used for the needed authentication in security systems. Besides, existing voice and video call subsystems or external communication (like usual phones) can be applied whenever additional security is indispensable.

The situation drastically changes in the two other scenarios. Although the user may even see each other face by face and have different interaction opportunities over a longer interval see [1], the relations mostly remain superficial. It is a fact, that only very few members of the second user group meet in real life.

Usually, public and private keys, digital signatures, certificates etc. may ensure in case 2) and 3) only that we meet always the same *registered person(s)*, (i.e. solve the problem of formal authentication and privacy), but it can even not ensure without additional measures that the user behind the computer is the always the same. Nevertheless, the main reason is to be seen in a deep problem to establish trust over a social network. And: it is hard to trick out the brain in this point, i.e. to force the brain to trust anyone.

A plenty of psychological and sociological publications deal with the complex problem of understanding trust [2] and to distinguish different human approaches to that depending on aspects of the character of the respective person [3]. It becomes clear that trust is not a fixed value but a parameter changing over time depending on very subjective rules and also non-explainable feelings. Even chemistry (smells) may play an important role in this process [4]. From the psychological point of view it must be accepted that users may obtain trust by fraud and that not every intelligently prepared plan may be recognised: in real life as well as in computer based OSN.

[5] figured out that trust building and trust estimation require long time, i.e. need a longer time of mutual communication and activities involving interactions in the social networks as well as in reality. The reason is that in this case the cost for any fraud is usually higher than the obtain reward of deception. Nevertheless, a single, accidently made lie may disrupt any friendship and destroy built trust suddenly with no chance for a later recovery [6].

If it is assumed that the behaviour of an individual is more or less rational and a constant one over a longer period, the consideration of the history gives the possibility to predict future activities. In such a manner, trust can be mostly understood a the predictability of activities of the other users in the respective environment.

Last but not least, it must be recognised that trust strongly depends on sociological factors, i.e the position in the social hierarchy of all persons, recommendation of other people (friends as well as strangers) and the estima-

tions of persons in the closest environment (family, team etc.). Such effects are already addressed in works on the *wisdom of crowds* [7] and the *word of mouth* [8]. Kleinberg motivates in his works on triadic closure [9] that two people are more likely to be friends or trust each other, if they share a mutual friend or highly appreciated person. The strength of the ties between the persons may influence the respective probability to establish a new friendship or trust relation.

From the above said, it becomes clear that trust estimation is a central point in future OSN.

2. Local Trust and User Activities

2.1. Successive Data Collection

Differing from the human approach of trust building, a technical system must be based on exact measurements of suitable parameters and algorithms as well as on how to combine them to a reliable trust value. In [1], we have discussed a first set of activities available for doing so in OSN.

The appearance of communication activities is the strongest instrument to evaluate the relation among two users. Hereby, communication includes not only the content of messages but also any other measurable parameters of communication like its time, frequency, duration etc. but also annotation of messages, e.g. if users *like* a posting, comment a posting or even mail to the user. Those parameters are more easy to measure than content aspects and may even be compared concerning their importance by weights.

Later, those numbers will be referred to as cumulative trust value between two users, i.e., user u_x trusts user u_y to a certain extent, denoted as $T(u_x, u_y)$. Note at this point that trust is not a symmetric relation, i.e. $T(u_x, u_y) \neq T(u_y, u_x)$ and subject to a permanent evaluation.

In detail, the following rules apply to generate a cumulative trust value $T(u_x, u_y)$ over the continuous interactions and activities with other users for a longer period of time.

For the special example of *Google+* the following rules were derived.

1. Being liked from a user u_x will increase $T(u_x, u_y)$.
2. Frequent, consecutive like activities may increase the trust value over time.
3. Positive comments have a more intense, increasing effect as likes. Note, that in this case the content must be analysed.
4. Being added as friend or receiving eMail from another user is also a quite positive signal, which result in an increased trust value.
5. Reaching a given trust value $T_f(u_x, u_y)$ will result in adding u_y as friend by u_x;
6. In the same manner a much lower value of $T_{uf}(u_x, u_y)$ may result in an 'unfriend'-activity.
7. Finding a triadic closure i.e. if u_x is friend of u_y and recognizing that u_y and u_z are friends, may increase the trust $T(u_x, u_z)$.
8. Also, a new friend may be randomly added with a small probability, representing a new friend from the real world. For those people, a starting trust value must be interactively determined.
9. Recognised lies will result in set $T(u_x, u_y)$ to zero. Consecutive activities (e.g. Unfriend) may depend on the users character.

Finally, it must be considered whether activities shall be valid over all time or for a specific time slice only, e.g. by using a (sliding) window approach.

Therefore, it can be assumed that an exponential oblivion process models the human thinking in the best manner. The local trust value $T(u_x, u_y)$ depend now on the time, i.e. becomes $T(u_x, u_y, t)$, where t is a discrete time step. If ${}_{\Delta}T(u_x, u_y, n+1)$ denotes the local trust changes obtained in the last time interval from n until $(n+1)$, $T(u_x, u_y, (n+1))$ can be calculated in a recursive manner without keeping all history values of $T(u_x, u_y, t)$ in the memory by:

$$T(u_x, u_y, (n+1)) = T(u_x, u_y, n)e^{-\lambda} + \frac{{}_{\Delta}T(u_x, u_y, (n+1))}{S}, \quad (1)$$

wherein λ is constant to determine the size of the window and S can be understood as the number of considered (weighted) values and can be counted by

$$S = \sum_{k=0}^{\infty} e^{-\lambda k} = \frac{1}{1 - e^{-\lambda}}. \quad (2)$$

Currently, a concrete quantitative analysis of trust alterations of $T(u_x, u_y)$ is not given in this article. These values, however, must be later empirically derived by experiments with a bigger group of users and be confirmed in a simulation process.

2.2. Generating Pairwise Trust

From human psychology it is clear, that the transition between no and full trust is definitely not a linear function, but more or less a sigmoid dependency, if few exceptional events resulting in an immediate loss of trust are not considered at the moment.

1. In the beginning, the first activities of a user are not adequately recognised for trust calculation.
2. After some time of doubt, positive activities result in a significant increase of trust.
3. When a time of probation is over, full trust is given.
4. This process, however, is reversible.

5. Some activities may result in an immediate loss of trust, this may be modeled again with a small probability $p_{lie}(u_x, u_y)$ representing that u_x is cheated by u_y such that any trust is destroyed and $T(u_x, u_y) = 0$.

As the linear combination of activities influencing the trust value of user u_x for user u_y is aggregated in $T(u_x, u_y)$, which can vary in a big range, normalisation should be introduced to map $T(u_x, u_y)$ to $t(u_x, u_y)$ with values in an interval of [0,1] following [10], which preserves the underlying trust semantics. The question is now how $t(u_x, u_y)$ can be suitably derived from $T(u_x, u_y)$?

A sigmoid function is often used and the suggested solution for our propose:

$$t(u_x, u_y) = \frac{1}{2} + \frac{T(u_x, u_y) - T_{off}}{2\sqrt{1 + (T(u_x, u_y) - T_{off})^2}}, \qquad (3)$$

whereby T_{off} describes the user characteristics, i.e. how much initial trust is given and how much positive activities must be performed in order to obtain an increased trust value.

Now, the pairwise trust functions must be used to generate a (global) trust value for each user, which shall not solely depend on a special pairwise business relation but be an overall trust evaluation of this user in his (complex) network of relations.

2.3. Global Trust and Random Walks

From the above said, it becomes clear that the (global) trust value of a user depends on the trust of all users knowing that user as well as the trustworthiness of those users. E.g. if a user A trusts a user B with 100 percent and has an own trust estimation of 10 percent only, this user probably cannot convince the community that B is reliable.

By considering those relations, the similarity to the calculation of PageRank [11] is highly visible. Indeed, the results of [12] show that we can use and specify the PageRank calculation for our needs. The advantage is that it is known that the PageRank of a node can be obtained by a fully decentralised working, random walker based method. Using these methodology, a global TrustScore $TS_{u_x}(t)$ is now easy to calculate in an iterative process which converge fast if k random walkers are used.

It is clear that the counted trust value $TS(u_x)$ is still a value, which depends on the network size, i.e. the bigger the network is, the smaller all values are. In order to make these values comparable, different normalization methods can be applied using the size of the network or relative measures.

3. Simulation

3.1. Simulation Setup

A check for performance and feasibility of the above concept through was done by a simplified Java multi-threads simulator of the real-time scenario.

The simulated social networks are firstly generated the Watts-Strogatz method [13] as directed graph with network size n, mean degree $k = 6$ and and a rewire probability $p = 0.5$. The trust values are weights of the edges obtained by the Richardson technique [14] as mentioned in [1]. Additionally, a massive dataset from real social networking are used in our simulation such as below trust networks directed weighted Advogato (6,541 users and 51,127 trust statements).

Convergence of whole TrustScore process is assumed if the difference between 2 consecutive states is acceptably small, i.e. 4.10^{-8} or lower.

3.2. Result and Discussion

Consequently, the result in Fig. 1 reveals that the distribution of TrustScore comply Gaussian distribution patterns. It can be seen that highest density of nodes is obtained in (0.150; 0.175].

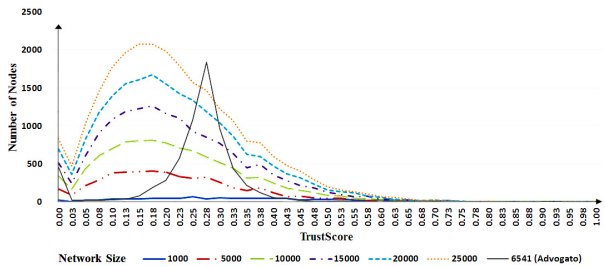

Figure 1: TrustScore distribution on simulated trust network in different size

Judging from statistics data in Fig. 1 on Advogato, Gaussian distribution remains and 1,842 nodes out of 6,541 nodes (28.16%) have mostly trust value in interval (0.25; 0.275].

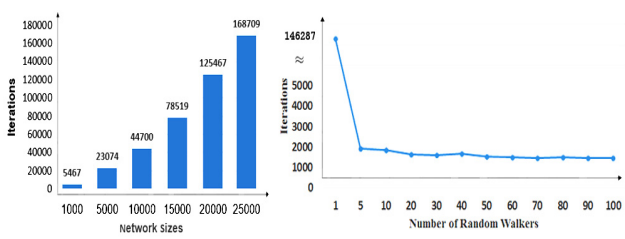

Figure 2: (a) Convergence in different network sizes (b) Convergence in restriction of number of random walkers

It follows from Fig. 2. a. that convergence in direct trust networks with different sizes increase steadily with regard to iterations.

In Fig. 2. b, the number of random walks was increased to be {1, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100}, respectively in order to accelerate convergence by parallel processing. Our simulation is implemented on simulated

Watts Strogatz network mentioned in subsection 3.1 with the network sizes 1,000 nodes. The experiment could be concluded that population of random walkers have effect on the convergence time. Obviously, the more random walkers TrustScore algorithm got, the earlier convergence it obtained. As we see, when number of random walkers is greater than 40, more exactly, parameter of restriction setting exceeds mean of population size then time convergence is quite stable. In fact, the calculation process may take a while, even if unlimited number of random walkers (100 and so forth) are used.

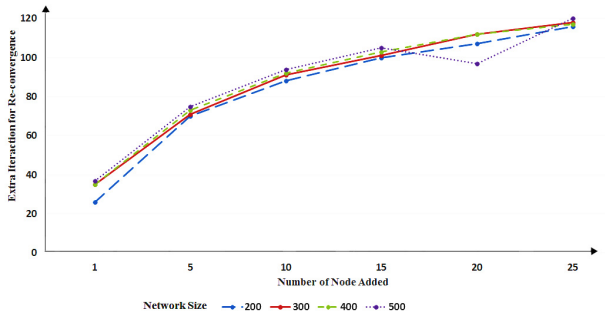

Figure 3: Re-convergence time with 1, 5, 10, 15, 20, 25 newly added nodes

Investigation of re-convergence with dynamic structure of topology is implemented through newly added 1, 5, 10, 15, 20 or 25 nodes with different network sizes in Fig. 3. The question is how many time TrustScore get new stable state after some new nodes join the network. It seems fairly difficult to catch characteristics of re-convergence, but general trend of re-convergence time is that the more newly nodes join the more time we need. Even size of network is different, but extra time for re-convergence corresponding number of newly added nodes seem slightly in parity. A trivial result is recognized that topology shape of network might have an effect on convergence rate beyond network size.

Our results of trust simulation were shown that TrustScore is sound and feasible. In future articles, the authors will take content into account for investigating influence of user-generated content on social network to trust.

4. Conclusion and Outlook

A fully decentralised concept to calculate global trust in an OSN was introduced. It is based on the evaluation of the predictability of user activities and uses random walkers for all communication and calculation processes. After a short startup time, trust values can be derived for every user, even when the information available on a particular user (e.g. when the user just joined the network) is sparse. In such a manner, the concept may contribute to endeavours to make online trading more safe. First experiments have been conducted and proved the practicability of the new concept.

References

[1] T.S. Doan, M. Kubek, “A Concept for Trust Derivation from User Activities”. Accepted on International Conference on Computing and Information Technology, 2015.

[2] M. Deutsch, “The resolution of conflict”. New Haven and London: Yale University Press, 1973.

[3] H.-G. Häusel, “Think Limbic”. Haufe Publisher, ISBN: 978-3-648-05883-1, 2014.

[4] A. Damasio, “Human behaviour: Brain trust”. Nature, Vol. 435, No. 7042, 571–572, 2005.

[5] H. Unger, T. Bohme, “A decentralized, probabilistic money system for P2P network communities”. In: Proceedings of the Virtual Goods Workshop, Ilmenau, 60–69, 2003.

[6] D.-G. Myers, “Psychology, 9th Edition. In Modules (Loose Leaf)”. Worth Publishers, ISBN: 1429277696, 9781429277693, 778p, 2010.

[7] J. Surowiecki, “The Wisdom of Crowds”. Anchor Publisher, ISBN: 0385721706, 2005.

[8] C. Dellarocas, “The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms”. Management Science 49 (10), 1407–1424, 2003.

[9] D. Easley, J. Kleinberg, “Networks, Crowds, and Markets: Reasoning About a Highly Connected World”. Cambridge University Press, 2010.

[10] S.P. Marsh, “Formalising Trust as a Computational Concept”. PhD thesis, University of Stirling, 1994.

[11] L. Page, S. Brin, R. Motwani and T. Winograd, “The pagerank citation ranking: Bringing order to the Web”. Technical Report, Stanford Digital Library Technologies Project, 1998.

[12] S. Sodsee, “Placing Files on the Nodes of Perr-to-Peer Systems”. PhD thesis, Fernuniversitat in Hagen, published in VDI Fortschrittsberichte Informatik, ISBN: 978-3-18-381610-1, Volume 218, Dusseldorf, 2012.

[13] D. Watts, S. Strogatz, “Collective dynamics of small-world networks”. Nature (393), 440–442, 1998.

[14] M. Richardson, R. Agrawal, P. Domingos, “Trust Management for the Semantic Web”. International Semantic Web Conference 2003, Springer-Verlag, 351–368, 2003.