A Concept for Trust Derivation from User Activities

Doan Trung Son and Mario Kubek

University in Hagen,
Faculty of Mathematics and Computer Science, Hagen, Germany
{doan.trung.son.vn,dr.mario.kubek}@gmail.com

Abstract. Business activities are usually based on trust and reputation of the participating actors. Online social networks present to their members manifold possibilities to meet new business partners, while an evaluation of their trustworthiness is still a quite unsafe and risky matter. Basing on communication activities, a new concept to obtain reliable trust values for any two users is introduced and its generalisation to a global, network wide trust system will be proposed. Last but not least, a fully decentralised processing for those trust values is proposed.

Keywords: trust, social networks, user activity, random walk, pagerank.

1 Introduction

In online businesses, security and trust are the most important factors for merchants and customers to protect their goods, money and transaction data from any unwanted loss. Recently, online social networks (ONS) became a huge marketplace [1], where people meet, negotiate, buy and sell any kind of products. Usually, those people never met before and rely on honesty and trustworthiness of the respective business partners. Of course, those media also attract people that intend to use them in an unhonest and unlawful manner. Consequently, the problem of distinguishing honest business partners from others such as cheating people appears [2]. While the problem of secure communications and transactions is quite well addressed by a series of cryptographic methods and protocols [3], the problem of giving trust to somebody is still an open problem, especially if people have never met in real life.

Trust can be understood as the reputation of people, i.e. the overall quality of character seen or judged by people in general [4]. It becomes clear that it will be quite hard to measure this by any quantitative values.

In [5] was figured out that a reliable trust estimation can be derived over a longer observation period, only, i.e. it requires a longer time of mutual communication and activities involving interactions in the social networks as well as in reality. Hereby, trust can be mostly understood a the predictability of activities of the other users in the respective environment. While it is relatively easy to determine the predictability of a limited number of activities of a user and measure

H. Unger et al. (eds.), *Recent Advances in Information and Communication Technology 2015*, Advances in Intelligent Systems and Computing 361, DOI: 10.1007/978-3-319-19024-2_17

it by a percentage value over a longer period, it is quite difficult to generate such a value at the first short term contact merchants and customer usually have. Recently, most merchants rely on customer evaluation on their web pages or evaluation activities of third parties, which still presents a lot of possibilities for manipulations [6]. The evaluation of the customer remains usually hidden and is done in the form of (secret) black lists of the merchants or groups of them. Consequently, it is intended to generalise the concept of *trust chains* such that from the pairwise trust values and the structure of the whole network a more or less objective trust value which is also protected against manipulation for each user can be derived.

In the following sections, a new concept for trust derivation shall be introduced, basing on the frequent use of online social networks. First, the generation of mutual trust between any two users is described in sec. 2. In sec. 3 shall be shown, how that pairwise trust estimation can be combined with the estimations of other users to a global trust value for all participants using a random walker approach. Last but not least, a concept for an implementation and a simulation setup is given.

2 Pairwise Trust of OSN-Users

Several psychological and sociological publications deal with the problem of understanding trust [7] [8][9][10]. It becomes clear that trust is not a fixed value but a parameter changing over time depending on very subjective rules and also feelings. Normally, user are carefully in the beginning, slowly gain trust until they fully believe in each other. Of course, this growth process may be durable and suddenly disturbed, if one of the partners occurs unreliable, e.g. by a single lie. From our point of view and following [5], trust might be quantified. 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. For the communication of users and the exchange of contents, users of OSNs may use a limited set of activities. A user usually can or has to

- register and establish a profile showing his interests (respectively content or information he offers or is looking for);
- establish, add or eventually remove friends (from the set of other OSN users), eventually divided into groups (note that the friendship relation is not in all systems a symmetric one, i.e. in some systems, A can be a friend of B without B being a friend of A);
- read, write (post) and redistribute content from other users while sometimes the system adds any new items to this set;
- communicate with other users by like (FaceBook), +1 (Google+) or other operations, comment their contributions or mail with them;
- establish groups or communities, which are a broadcast possibility for their members to all other members.

While it is hard to analyse the content of a OSN, the appearance of communication activities is a strong instrument to evaluate the relation among two users. Moreover, posting or communicating some content is published with the expectation to obtain some reward, i.e. like's of those content, comments, mail etc. In such a manner, some relations of cause and impact appear with every activity in a OSN, which can be measured, predicted and evaluated condering their frequency by real numbers. Those numbers later 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. $T(u_x, u_y) \neq T(u_y, u_x)$.

Summarizing our understanding means that the trust $T(u_x, u_y)$ between any two users u_x and u_y mostly depends on:

1. the time the two users know each other,
2. the similarity of their interests,
3. the mutual predictability of their activities and last but not least,
4. some (often initially given) mutual sympathy (which is of course hard to model).

Being a friend (note that we use the term in business and private matters, although it is usually called a partner in business) is in both real world and social networks a special expression of trust and subject to a permanent evaluation.

Trust non-monotonically and dynamically changes and is adapted to the changing conditions of contexts, in which user activities take place. Of course, also external, real-world influences effect users' trust and may result in a rapid increase or decrease of the trust value among any two users.

In the described approach, (only) the above activities will be used to cause a (periodical) increase or decrease of trust between any pair of users starting from an initially given trust $T_0(u_x, u_y)$, which depends on hardly predictable personal circumstances and preferences.

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. Positive comments have a more intense, increasing effect as likes.
3. If u_y posts interesting (i.e. usually similar) content, which u_x reads, it will increase $T(u_x, u_y)$. Frequent, consecutive like activities may increase the trust value stronger over time.
4. Posting uninteresting, offending content will decrease $T(u_x, u_y)$, especially (and therefore in an exponential manner) if it happens in an uninterrupted series.
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. recognizing that u_y and u_z are friends, may increase the trust $T(u_x, u_z)$. A differentiation using strong and weak ties may be also useful.
8. Also, a new friend may be randomly added with a small probability, representing a new friend from the real world.

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 and be confirmed in a simulation process.

From the 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].

1. In the beginning, the first activities of a users are not adequately recognised.
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 $T(u_x, u_y) = 0$.
6. It must be discussed whether activities shall be considered over all time using e.g. a (sliding) window approach or for a specific time slice only.

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 [11], 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 [12] and the suggested solution for our propose:

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

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.

[1] Lies are an important strategic possibility of individuals in society to reach their goals.

3 Random Walks-Based Trust Calculation

From the above said, it becomes clear that the (global) trust value of a user depends on on the trust of all users knowing him as well as the trustworthiness of those users. E.g. if a user A trust 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 [13] is highly visible. Indeed, the results of [14] show that we can use and specify the PageRank calculation for our needs. Another advantage is that it is known that the PageRank of a node can be obtained by a fully decentralised working, random walker based method.

While PageRank reflects — as intended in the before cited original publication — only topological aspects of nodes embedded into (web-) graphs, [14] includes other factors generating graphs with weighted edges in other words continuous-valued networks, which may influence the role of a node in a system. Originally, the transition probability of a random walker from a node u_x to a node u_y $p(v_x, v_y) = \frac{1}{|N_u|}$ is the only parameter influencing the PageRank besides the topological properties of the underlying graph.

In order to obtain a TrustRank TR, the global trust value for each node in a complex OSN, the trust values $t(u_x, u_y)$ can be used, i.e. the trust a user u_x has in another user u_y. With this assumption, the transition probability of a random walker to move from v_x to v_y can be defined as

$$p(v_x, v_y) = \frac{t(u_x, u_y)}{\sum_{\forall u_a \in |N_{u_x}|} t(u_x, u_a)}, \tag{2}$$

where $\sum_{u_a \in N_{u_x}} p(v_x, v_a) = 1$. It is easy to see that now the random walker will prefer links with a higher trust.

The TrustRank is now easy to calculate and can be obtained faster by using k random walkers.

If $k \in \mathbf{N}$ random walkers are used, then the TrustRank can be calculated by

$$TR_{u_x}(t) = \frac{\sum_{\forall k} f_{u_{x_k}}(t)}{\sum_{\forall k} step_k(t)}, \tag{3}$$

where $f_{u_{x_k}}(t)$ is the number of all visits of the k-th random walker on u_x so far in all its $step_k(t)$ steps until time t.

It is clear that the counted trust value $TR(u_x)$ 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, a normalization must be carried out using the size of the network. For centralized OSN, this value is known to the provider.

For any other cases, [14] suggests a small trick using a property of mean values which helps to cope with this situation, viz. the mean value of a small number of samples already approximates the real mean value normally quite well. Based on

the knowledge above and some basic mathematics it is known that the average TrustRank of all nodes in a community $\overline{TR}$ is given by

$$\overline{TR} = \frac{\sum_i TR_i}{n} = \frac{1}{n}. \tag{4}$$

Hence, to calculate the average TrustRank, n can be estimated from a smaller number of samples than by considering the entire number of nodes by

$$n = \frac{\sum_{i=1(1)K} TR_i}{\overline{TR}} = \frac{1}{\overline{TR}}, \tag{5}$$

with $K < |V|$. In other words, the network size is estimated from a sample of TR values whose mean value will converge to $\frac{1}{n}$. Now, only a good estimation for K is needed. This can be replaced, however, by considering the deviation of the calculated mean value. The calculation can be stopped when the deviation is small enough and/or the mean value is stable enough.

With the above method, a trustworthiness of a node u_y can be counted from the trust, any user u_x gives to that node by $t(u_x, u_y)$. Since this value will be kept on u_y, the question on possibilities of its manipulation comes up. In [5], a protocol is introduced to check the validity of an (electronic) coin by keeping it on a set of previous machines and checking those history information.

A similar approach can be used for the trust values. Hereby, a random walker carries the just counted trust value $TR(u_x)$ with him and distributes it on the s next nodes on his way. After some time, all possible successors will have an (almost) correct value of $TR(u_x)$. This value can therefore be obtained from any (doubting) node accessing u_x by visiting those nodes that are reachable within s steps from u_x. This method works correctly as long as u_x cannot allocate and manipulate a larger number of nodes (how much depends on s and the out-degree of its successor nodes).

Last but not least, it shall be mentioned that the security mechanism from [5] may be applied to avoid any manipulation of the trust values by the user. It is mainly based on the propagation of the trust values along a randomly chosen trail through the network and the selection of a (smaller) group of nodes as witnesses for the confirmation of the respective locally stored value.

4 Simulation and Implementation

So far, only a limited, small simulation has been setup to prove the described concept. It contains the simulation of just 200 nodes in a small-world network generated by the algorithm introduced by Watts and Strogatz [15].

Since we do not have an ONS to obtain realistic user data in the first version of simulation, the initialisation has to also include the generation of trust weights for the edges of the network. Therefore the Richardson technique [16] is applied to uniformly choose a continuous value for the directed edges between two nodes u_x and u_y in scaled intervals $[max(\gamma_{u_y} - \varphi_{u_x u_y}, 0), min(\gamma_{u_y} + \varphi_{u_x u_y}, 1)]$, while

the quality parameter γ_{u_y} was chosen from Gaussian distribution with $\mu = 0.5$ and $\delta = 0.25$; the noise parameter $\varphi_{u_x u_y}$ has been set to $1 - \gamma_{u_y}$.

The first experiments had the goal to prove that

1. random walkers are a suitable tool to calculate the PageRank of nodes in complex networks and to obtain an idea of the speed of convergence and
2. a realistic distribution of trust values can be obtained.

For both goals, satisfying results could be achieved. Fig. 1 shows once more that the euclidean distance between the values obtained from PageRank and the Random walks-based method converges to zero indicating that both algorithms are quite strongly correlated. If the number of iterations is big enough (i.e. $\geq$ 2.000 iterations), the result reveals an acceptably small distance of around 0.008. The results, however, still do not cover real-world conditions with a large number of nodes involved. Also, the number of needed steps to achieve convergence is quite high such that mechanisms are needed to improve the convergence speed.

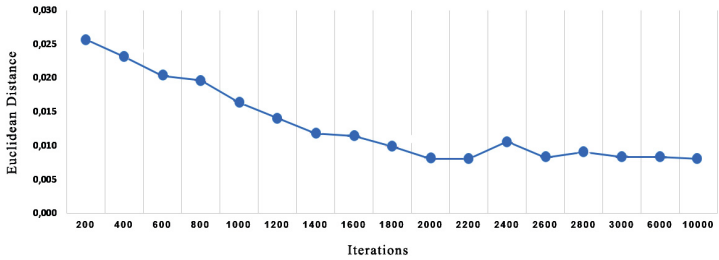

Fig. 1. Euclidean distance correlation between Page Rank and Random walks-based method on binary-valued networks

Good results could also be obtained from the statistics of the obtained trust rank in Fig. 2. It is worth to point out that the TrustRank values follow a gaussian distribution. Additionally, the simulation result of TrustRank shows the mean value of users' (not normalised) TrustRank $\overline{TR}$ of 0.0049855 after 10.000 iterations. It also shows that the summation of all values amounts to TR 0.9971, which is approximately equal to 1, which is fairly suitable according to the theoretic statements given in the previous section.

In Fig. 3 the intended implementation of the developed trust management system is shown in the context of any OSN, in our case *Google+*.

It is to be seen that the suggested system mostly consists of an application running in parallel to the OSN. It is able to collect data from the social network, in particular it can access any neighbourhood (friendship) information of a particular user and record all its activities (since this happens locally on the user's computer, no security concerns may arise). From those activities, the respective pairwise, local trust values can be calculated.

In addition, the application contains a management system for a population of random walkers, controlled as suggested in the literature by [5], [14]. The random

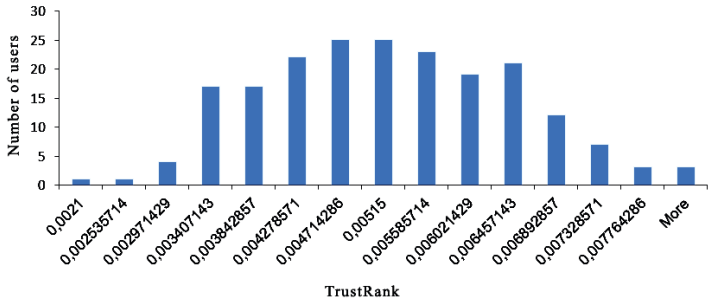

Fig. 2. Distribution of $TrustRank$ values of two hundreds of users

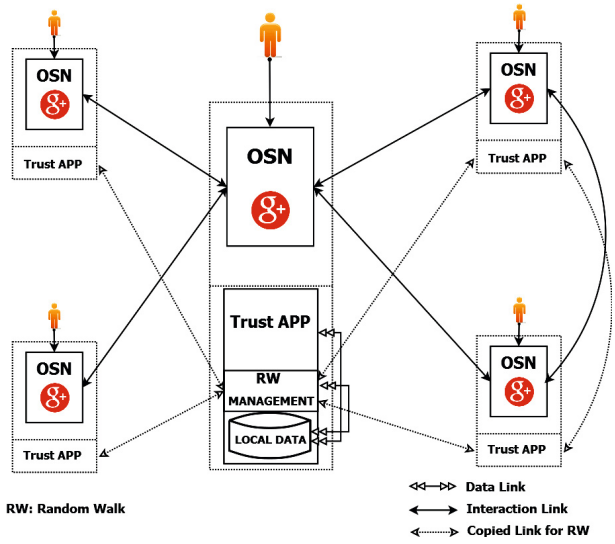

Fig. 3. Blockscheme of the intended trust management system

walkers may follow the copied links of the OSN and generate the global trust values for the users. In addition, those trust values are copied along a random trail in order to avoid unwanted manipulations as described above.

5 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 to prove the technical soundness of this concept.

In future works, larger simulations will be carried out and an implementation embedded in a real OSN environment along with its test results will be provided to obtain more detailed information about the dynamics and reliability of the proposed mechanisms including a study of its practicability in the daily use.

References

1. Easley, D., Kleinberg, J.: Networks, Crowds, and Markets: Reasoning About a Highly Connected World. Cambridge University Press (2010)
2. Mazar, N., Amir, O., Ariely, D.: The Dishonesty of Honest People: A Theory of Self-Concept Maintenance Social Science Research Network Working Paper Series (2007)
3. Liu, C., Marchewka, J.T., Lu, J., Yu, C.S.: Beyond concern: a privacy-trust-behavioral intention model of electronic commerce. Information and Management 42(1), 127–142 (2004)
4. Jøsang, A.: Trust and Reputation Systems. In: Aldini, A., Gorrieri, R. (eds.) FOSAD 2007. LNCS, vol. 4677, pp. 209–245. Springer, Heidelberg (2007)
5. Unger, H., Bohme, T.: A decentralized, probabilistic money system for P2P network communities. In: Proceedings of the Virtual Goods Workshop, Ilmenau, pp. 60–69 (2003)
6. Jøsang, A., Golbeck, J.: Challenges for robust of trust and reputation systems. In: Proceeding of the 5th International Workshop on Security and Trust Management (2009)
7. Deutsch, M.: The resolution of conflict. Yale University Press, New Haven, London (1973)
8. Grabner-Kräuter, S., Kaluscha, E.A.: Empirical research in on-line trust: a review and critical assessment. Int. J. Hum.-Comput. Stud. 58(6), 783–812 (2003)
9. McKnight, D.H., Choudhury, V., Kacmar, C.J.: Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. Information Systems Research 13(3), 334–359 (2002)
10. McKnight, D.H., Chervany, N.L.: The Meanings of Trust. UMN university report (2003)
11. Marsh, S.P.: Formalising Trust as a Computational Concept. PhD thesis, University of Stirling (1994)
12. Gibbs, M.N., MacKay, D.J.C.: Variational Gaussian process classifiers. IEEE Trans. Neural Netw. Learning Syst. 11(6), 1458–1464 (2000)
13. Page, L., Brin, S., Motwani, R., Winograd, T.: The pagerank citation ranking: Bringing order to the web. Technical Report, Stanford Digital Library Technologies Project (1998)
14. Sodsee, S.: Placing Files on the Nodes of Perr-to-Peer Systems. PhD thesis, Fernuniversitat in Hagen, published in VDI Fortschrittsberichte Informatik, Dusseldorf, vol. 218 (2012) ISBN: 978-3-18-381610-1
15. Watts, D., Strogatz, S.: Collective dynamics of small-world networks. Nature (393), 440–442 (1998)
16. Richardson, M., Agrawal, R., Domingos, P.: Trust Management for the Semantic Web. In: Fensel, D., Sycara, K., Mylopoulos, J. (eds.) ISWC 2003. LNCS, vol. 2870, pp. 351–368. Springer, Heidelberg (2003)