CHARACTERISTICS OF TRUST IN ONLINE SOCIAL NETWORKS AND COMMUNITY OF TRUST AS A SPECIAL CASE OF ONLINE COMMUNITY

David Zejda
Faculty of Informatics and Management, University of Hradec Králové, Hradec Králové, Czech Republic

Keywords: Trust, Distrust, Community of trust, Social networks, Community.

Abstract: With boost of interest in Web 2.0 technologies, appropriate trust models are increasingly more important. First section the paper contains state of the art about trust characteristics, in particular multidimensionality, contextuality, scope of relevance, transitivity and asymmetry. Transitivity as a key aspect utilized in most models is described in a slightly greater detail. Discussion on scope of relevance allowed us to introduce taxonomy of trust from the scope point of view. Based on the general foundation, in the second section we introduce community of trust as a niche type of online community where users trust each other as default and where the trust loses most of its subjective flavour.

1 INTRODUCTION

Both individual social interactions and a whole dynamics of personal social network are highly influenced by trust. Trust may be defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party." (Mayer et al., 1995) For our work we adopted rather the definition: "Trust in a person is a commitment to an action based on a belief that the future actions of that person will lead to a good outcome." (Golbeck & Hendler, 2006) The level of trust which we feel toward someone helps us to decide whether to rely on his promises or whether to entrust him an information or a task.

Trust emerges primarily from our experiences with others, their acts, words, their willingness to help us in difficulties, promises which have been kept. Another source of trust is recommendation or guarantee from those, who we trust already. In general, trust grows slowly, but falls sharply. (Walter et al., 2008) It may take months or years before we credit someone, whereas a single act of betrayal destroys the trust from the roots.

We all belong to a global-world village. As expressed in the small world phenomenon, everyone is connected with anyone else through only several steps of relations. (Pavlovic, 2009) Current technology emphasizes the connectedness. Besides milieu for implicit socialization (Wennerberg & Oellinger, 2006), web provides variety of explicitly social spaces, including dating sites, community portals and social networking sites. If we add pace of life nowadays, new social strategies are needed to cope with the social and information overload. (Walter et al., 2008) Reliable, efficient, and appropriate trust solutions for social software should reflect the needs. In the paper we present state of the art about trust characteristics and define community of trust as a niche kind of community where trust among users is a default state.

2 TRUST CHARACTERISTICS

Online interactions may be viewed as a technical extension of interactions in real world. (Dwyer et al., 2007) So, trust in online networking systems keeps most of its general characteristics. Meo et al. (Meo et al., 2009) define three aspects of trust, multidimensionality, contextuality and scope of relevance. Goldbeck et al. identify transitivity, asymmetry and personalization (Golbeck & Hendler, 2006). Personalization may be viewed as a special case of scope of relevance. We decided to add disproportion of impacts and dynamics.

Zejda D..
CHARACTERISTICS OF TRUST IN ONLINE SOCIAL NETWORKS AND COMMUNITY OF TRUST AS A SPECIAL CASE OF ONLINE COMMUNITY.
DOI: 10.5220/0003332905310534
In *Proceedings of the 7th International Conference on Web Information Systems and Technologies* (WEBIST-2011), pages 531-534
ISBN: 978-989-8425-51-5

Multidimensionality. There is no single source of trust, on the contrary various factors may be considered to evaluate trust, such as honesty, experience, precision, efficiency, or cooperativeness of the party. We may mix the indices to get more complex view. Dimensions grow with breadth of a social network. In a virtual space on one hand we miss non-verbal indices. We do not see others in real, sometimes even not at all. It is also likely that there are not many trustful people around who could share their real world experiences. On the other hand we may take the whole community into account and use plenty of algorithms to overcome the drawback.

Contextuality. Social context and purpose of trust evaluation affect our requirements on trust and the process of trust formation - trust is contextually-dependant. E.g. when we search for advices on particular topic, we prefer experts on the domain.

Asymmetry. Trust of one to another does not imply trust in reverse direction. Graph of trust is directed, matrix of trust is not necessarily symmetrical.

Transitivity. Admitting transitivity of trust, we may follow trust relations to infer trust between those who do not trust each other yet or who even do not know each other. Multiplication along the path performed by most algorithms effectively discounts the resulting value (Huang & Fox 2006), thus those whom the user trusts already are being taken more seriously as a source of recommendations whom else to trust. The algorithms differ in their focus. E.g. some of them do not reduce cycles in a graph before computation (Walter et al. 2009) or may be applied in an environment with no central authority, e.g. to find cooperative routes among selfish agents acting as players in prisoner's dilemma. (Hales & Arteconi, 2005) Work on trust inference comprises e.g.: (Ziegler & Lausen, 2004) (Kamvar et al., 2003) (Guha et al., 2004) (Richardson et al. 2003).

Scope of relevance. It is necessary to distinguish subjective trust to objective trust. Many models treat trust as inherently subjective. (Golbeck & Hendler, 2006) Meo et al. classify subjective trust, community-wide reputation, and general reliability. (Meo et al., 2009) We further split reliability into system-wide trustfulness and world-wide trust identity exceeding borders of systems, as described in Figure 1. Trustworthy user is usually being trusted subjectively more quickly, reversely trustworthiness may be inferred from a set of subjective trust expressions. The inference my be performed with an eigenvector[1] algorithm, weighing subjective trust according to trustor's own trust. (Yan & Holtmanns, 2007). In result, trustworthiness of certain user stems from trustworthiness of his neighbours in the graph of trust (Walter et al., 2009). Explicit negative experiences (signs of subjective distrust) may help to reveal objectively malicious users. We lack applicable solutions for world-wide trust identity.

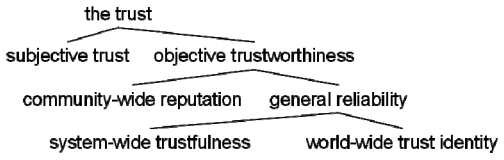

Figure 1: Taxonomy of trust.

Disproportion of impacts. We may identify two complementing types of errors in the process of trust emergence. The first is 'excessive prudence' when an user is excessively suspicious. The error inhibits formation of vital trust and lead to certain losses. On the contrary 'undue confidence' occurs if an user is either intentionally careless or if he is prone to fraud attempts. The second error may lead to more severe impacts, which should be reflected in trust models.

Dynamics. Caverlee at al. recommend to fold two main sources of information in a well-designed trust metric – network topology and record of behaviour. (Caverlee et al., 2008) Moghaddam et al. provide model for rapidly evolving networks, with puts emphasis on feedback as a source of trust. (Moghaddam et al., 2009) Driven by the dynamics, trust undergoes transitions between various states, it may be gained, lowered, or even lost. Conceptual representations of failures of trust, such as distrust, mistrust, untrust and ignorance are available. Trust may be recovered again, when regret followed by forgiveness takes place. (Golbeck, 2008)

The characteristics mentioned are mutually interrelated. E.g. contextuality brings further dynamics to the model, severity of impacts is further influenced by the context and scope of relevance, etc. Yan et al. reflect most of the characteristics in their conditional definition of trust: “Trustor A trusts trustee B for purpose P under condition C based on root trust R”. (Yan & Cofta, 2004) Trustor should be informed about any distrustful behaviour of the trustee according to the conditions and trust itself is considered as dependant on the conditions.

3 COMMUNITY OF TRUST

What's the source of trust in social networking systems? Trusted friendships may arise out of vital interactions within a site, usually during a sufficient

[1] Eigenvector-type algorithm is PageRank by Google.

period of time and based on a sufficient level of harmless activity. The model is meaningful for most cases, however, perception of virtue of trust is not unique among all communities. So, various models of trust are needed to reflect the needs.

Besides the trust which evolves with online interactions, also trust existing in a real social background may be mapped into an online system (Walter et al., 2008). For example, if you personally invite someone to join a networking site, you probably know him already and trust him, at least at certain degree. The trust has been established in advance already, based on your real world personal experiences. You do not ask the system to show you trustworthiness of the user. Rather reversely, you may provide trust indices to the system. If we follow the idea further, 'community of trust' is the scenario where users of certain online social system trust each other as default. Distrustful behaviour is rare there and if occurs, it leads to immediate expulsion from the community. Community of trust may exist among relatives, among close friends who know each other for a long time, among volunteers working jointly on an issue, among members of a church with strong influence on adherent's life or within another group of people bonded with strong shared principles. Table 1 outlines characteristics of community of trust, discussed in more detail below.

Table 1: Community of trust vs. a common community.

common community	**community of trust**
model of trust	model of distrust
distrustful behaviour relatively common	distrustful behaviour rare, propagate distrust quickly
users are notably cautious	users are careless
pre-validation of users not necessary / possible	users have to prove their membership first
users may express trust or both trust and distrust	users may express distrust or confirm trust
trust is important	trust is pivotal
trust is to be gained	trust is default state
trust is subjective	trust is objective
trust is dynamic	trust is not too dynamic
trust is transitive	distrust is totally transitive

While in online social networking systems supporting a common community we talk about a model of trust, in community of trust more appropriate name is model of distrust, because it fulfils different purposes. Primarily it helps to reveal intruders, impostors or those who turned bad. Besides the main purpose, the model of distrust indirectly fosters fair interactions within the community, bringing deeper feeling of reliance and connectedness. Healthful fear of possible consequences motivates users to adhere to the principles which keep the community together and to avoid any bad behaviour.

According to (Golbeck & Hendler, 2006) trust is a personal opinion, which means that each node has different levels of trust for each other node (Meo et al., 2009), but they admit, that systems based on objective trust may exist. Community of trust is the case. It is so tightly coupled that trust loses most of its subjective flavour and turns objective. As long as someone belongs to the community, others trust him. If he behaves badly to one, nobody will trust him more. Transitivity of distrust in a pure community of trust is total. So, while in subjective models of trust it gives sense to infer trust and distrust from a graph of trust relations following paths of transitivity, in community of trust it gives sense no more, because trust is default and transitivity of distrust tends to infinity. In most models, e.g. (Caverlee et al., 2008), trust is dynamic, reflecting changes in both network topology and activities of users. Model for community of trust is not too dynamic, but distrust has to be propagated as quickly as possible to the whole community.

Generally, people are willing to make only the effort, which brings obvious reward to them. Talking about trust or distrust models, users should be allowed to express their (dis)trust in situations and in a way which reflects their pattern of thinking or their habitual approach. The approach differs per context or per community. In community of trust users do not like to be annoyed with requests to evaluate trust with every transaction or to express trust of each other because trust is natural, implicit there. They only wish to have something at hand to defend themselves and the whole community if matters go wrong. Eventually they would also like to confirm the trust within the community to contribute to its virtue.

Any model of trust itself should be trusted by users, which implies that it should be also understandable. Because trust is so vital within a community of trust, it further underlines the requirement to bring appropriate model, and to keep it understandable. Users have to be authenticated first before entering a community of trust. Details of the validation process depend on a particular community and are out of scope of this paper.

4 CONCLUSIONS

In the paper we outlined state of the art trust

solutions for online social networks. Besides multidimensionality, contextuality, asymmetry, transitivity, scope of relevance, two more characteristics of trust have been identified - disproportion of impacts and trust dynamics. Subsequently we described basic ideas of trust processing and inference in models with transitive trust. Idea of scope of relevance has been extended into simple taxonomy of trust. As a main contribution, we introduced 'community of trust' to describe niche tightly coupled communities where trust among users is default state. Trust has objective character there, so tracking paths of trust among users has no sense. Model of distrust for community of trust has to propagate every distrust quickly to the whole community.

ACKNOWLEDGEMENTS

The research was supported by grant UHK FIM specific research 2110/2010.

REFERENCES

Caverlee, J., Liu, L. & Webb, S., 2008. Towards robust trust establishment in web-based social networks with socialtrust. In *Proceeding of the 17th conference on WWW*. Beijing, China: ACM, pp. 1163-1164.

Dwyer, C., Hiltz, S. & Passerini, K., 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *Proceedings of the Thirteenth Americas Conference on Information Systems*. Keystone, CO, USA.

Golbeck, J., 2008. Computing with Social Trust 1 ed., Springer.

Golbeck, J. & Hendler, J., 2006. Inferring binary trust relationships in Web-based social networks. *ACM Trans. Internet Technol.*, 6(4), pp.497-529.

Guha, R. et al., 2004. Propagation of trust and distrust. In *Proceedings of the 13th international conference on World Wide Web*. New York, NY, USA: ACM, pp. 403-412.

Hales, D. & Arteconi, S., 2005. Friends for Free: Self-Organizing Artificial Social Networks for Trust and Cooperation.

Huang, J. & Fox, M. S., 2006. An ontology of trust: formal semantics and transitivity. *In Proceedings of the 8th international conference on Electronic commerce*. Fredericton, New Brunswick, Canada: ACM, pp. 259-270.

Kamvar, S. D., Schlosser, M. T. & Garcia-Molina, H., 2003. The Eigentrust algorithm for reputation management in P2P networks. *In Proceedings of the 12th international conference on World Wide Web*. Budapest, Hungary: ACM, pp. 640-651.

Mayer, R., Davis, J. & Schoorman, D., 1995. An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3), pp.734, 709.

Meo, P. D. et al., 2009. Finding reliable users and social networks in a social internetworking system. *In Proceedings of the 2009 International Database Engineering & Applications Symposium*. Cetraro - Calabria, Italy: ACM, pp. 173-181.

Moghaddam, S. et al., 2009. FeedbackTrust: using feedback effects in trust-based recommendation systems. *In Proceedings of the third ACM conference on Recommender systems*. New York, New York, USA: ACM, pp. 269-272.

Pavlovic, D., 2009. Dynamics, Robustness and Fragility of Trust. *In Formal Aspects in Security and Trust: 5th International Workshop*, FAST 2008 Malaga, Spain, October 9-10, 2008 Revised Selected Papers. Springer-Verlag, pp. 97-113.

Richardson, M., Agrawal, R. & Domingos, P., 2003. Trust Management for the Semantic Web. *In The SemanticWeb - ISWC 2003*. pp. 351-368.

Walter, F., Battiston, S. & Schweitzer, F., 2008. A model of a trust-based recommendation system on a social network. *Autonomous Agents and Multi-Agent Systems*, 16(1), pp.57-74.

Walter, F. E., Battiston, S. & Schweitzer, F., 2009. Personalised and dynamic trust in social networks. In *Proceedings of the third ACM conference on Recommender systems*. New York, New York, USA: ACM, pp. 197-204.

Wennerberg, P. O. & Oellinger, T., 2006. Ontology Based Modelling and Visualization of Social Networks for the Web: Discovering Security Related Information from Online News Sites.

Yan, Z. & Cofta, P., 2004. A Mechanism for Trust Sustainability Among Trusted Computing Platforms. In Trust and Privacy in Digital Business. pp. 11-19.

Yan, Z. & Holtmanns, S., 2007. Trust Modeling and Management: from Social Trust to Digital Trust. book chapter of Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions.

Ziegler, C. & Lausen, G., 2004. Spreading Activation Models for Trust Propagation. *In Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service* (EEE'04). IEEE Computer Society, pp. 83-97.