Calculating Trust value in Information Propagation for Online Social Network Sites

Sanaz Kavianpour, Bharanidharan Shanmugam, Zuraini Ismail

***Abstract*— Trust concerns have increased dramatically by the augmentation of online social network sites (OSNSs) popularity. The worth of OSNSs is to form relationships and propagate social information from users' interactions which is beneficial for not only the users but inclusive of cooperator and business values. Thus, the question lies in creating architecture for the social network for communicating and disseminating information with trust as the central concern. The goal of this paper is to highlight and review trust importance in information dissemination for OSNSs. The findings lead to suggest trust level which can be applied on OSNSs to govern amount of information sharing. Hence, a new algorithm is proposed to calculate trust level for information dissemination.**

***Index Terms*— Information Propagation, Online Social Network Sites, privacy, trust.**

I. INTRODUCTION

Online social network sites (OSNSs) are highly attractive communication and information sharing services by the internet users [1]. OSNSs facilitate social interactions over distance and time. Individuals join these sites to communicate, to socialize [2] to make new friendships [3] and keep relationships with offline friends, share photos and videos, update events, send messages privately or publicly. Although these sites provide lots of merits for individuals, they cause some demerits such as unauthorized diffusing of private information, inadequate privacy settings, scalability and manageability because of the open and decentralized nature.

The OSNSs privacy vulnerabilities cannot be managed by users comprehensively due to insufficient privacy settings options provided by OSNSs, uninformed of the existing privacy settings, difficulty of usage, the only type of relationship (friendship make connection be-tween users), and inability to detect prospective privacy concerns because of untrustworthy friends. Friendship strength is a critical factor for people when deciding the frontier of their privacy in offline world. People consider different friendships in their offline world in order to control privacy threats in contrary with online world in which friendships are not well differentiated. Therefore,friendships on OSNSs may make privacy threats because of the lack of trust and acquaintance.

Trust is a complicated social phenomenon and a significant factor of social interactions [4]. It plays an important role in social network analysis as the nature of these sites is based on social interactions among users. Trust appears from experiences with people and advices from whom we trust already in real life. Level of trust from acquaintance is different from level of trust from strangers; accordingly trust is an important factor in making decisions to share content with proportional person.

Users' disclosed information and content need to be evaluated for trustworthiness. This could assist users to arrange and block undesirable information dissemination, make decisions and communicate with whom they have trust. According to Jøsang and Pope, if user A trusts user B and user B trusts user C, then user A can trust user C to some extent [5]. The best trust value among users can be calculated via extent trust that transit alongside with a social trust path that contains trust information which links the source and target users. Calculating trust because of its mediating function is a significant concern for scholars in computer interactions [6].

Hence, the aim of this study is to propose a new algorithm to calculate trust level for information dissemination. This paper proceeds with the definition on trust concepts in Section 2. Related works on trust are explained in Section 3. Trust model developments follow in Section 4. Evaluation of trust level in information diffusion is explained in Section 5. Section 6 concludes and provides the future work for this study.

II. TRUST CONCEPTS

A. Definition of Trust

Trust is an obscure concept which has been notably studied in psychology, philosophy, sociology and computer science. Mui et al. stated that trust is a subjective expectation of a user about other's future behavior based on the history of their encounters [7].

Jøsang presented trust by two generalized definitions as follows. Reliability trust which is known as evaluation trust, describes trust as the subjective probability by which a party (trustor) expects that another party (trustee) performs a given action on which its welfare depends. Decision trust is the extent to which trustor is willing to depend on trustee, in a given situation with a sense ofrelative security [8]. These definitions illustrate that dependency; risk and uncertainty are the main ingredients of trust. Diverse types of trust within the same target from various entities show that trust is subjective.

Manuscript received March 20, 2014

Sanaz Kavianpour,Advanced Informatics School (AIS),Universiti Teknologi Malaysia(UTM), Kuala Lumpur, Malaysia, 006-0129796978.

Bharanidharan Shanmugam, Advanced Informatics School (AIS), Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia.

Zuraini Ismail, Advanced Informatics School (AIS), Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia.

III. Trust Roles for Online Social Network Sites

Online social network sites provide virtual communities which form and use relationships. The relationships have binary value and they are different from real life relationships as they have various values [9]. Users are connected with relations on online social network sites. These relations are limited to being a friend or not on OSNSs; while in offline world (real life), these relations have various types such as close friends, relatives, business contacts, and so forth. Content, direction and strength are three attributes of each connection. The strength of a relationship indicates the intensity of a connection that depicts the closeness of two users [10]. On OSNSs, many users accept friend requests from those persons who do not know or do not have trust.

Trust is a vital part of the relationship between two users; and in a social network plays a significant role in the intelligence and security domain. The foundation of virtual communities is based on trust among the users in order to extended and be popular. Trust can detect influential users on social networks and control information dissemination. It is essential for online social interactions [11] as it has high effect on person's decision to what to share and with whom. Social trust affects information sharing by making a bridge for both interpersonal and social interactions. The growth of trust is related to the collection of behaviors and activities that have seen during a period of time, psychological perceives such as same ideas and sense of humor, sources of information or relationships [12].

In social network sites, users expect to receive both trust and distrust from other users' idea as they communicate vastly through these sites [7]. According to the Siegrist and Cvetkovich, users' decisions are typically guided by social trust as they are unable to develop trustworthy information about advantage and disadvantage of online technologies [13]. Based on electronic commerce research done in USA, trust has direct relation with information disclosure as it can decrease privacy concerns by preventing private information disclosure [14].

OSNSs trust level can vary from one user to another unlike offline [15], as each user can control a relation by deleting, accepting and communicating with others. However, trustee's trustworthiness is still the basic factor of both offline and online trusts. In comparing SNSs such as Facebook vs. MySpace, the result shows that Face-book users reveal more real information while the MySpace users' information are exaggerated according to the June Ahn research. It is found that MySpace users are more eager to make online relationships [16]. Most of the users believe that they are able to block or ignore the
messages, so they can decrease the privacy risk of making new relationship online although the trust is less [17]. Users of social network sites may give false information instead of real information especially in MySpace which may cause trust issues.

Hence, it is suggested that social trust is the main factor in interpersonal interaction as relationships can be formed just through trust. Social trust of a user may imply positive response for relationships and information exchange in OSNSs. By propagation of social trust, it is advocated that the number of social interactions will be increased.

IV. Related Works on Trust

A. *Trust Features*

Trust has several key features [18] [19] that have been identified by several researchers as follows.

Asymmetric. Trust level is not identical and does not have reverse direction. This means if person A trust person B 100%, person B may trust person A, just 50% and not completely 100%.

Transitive. Trust can be transit between those who have already known each other or who do not know each other; this may happen especially through virtual communities such as social network sites. Trust transitivity has direct relation with distance.

Personalized. Trust is subjective which means two entities may have various ideas about the same target trustworthiness.

Multidimensional. Trust evaluation depends on various factors such as experience, proficiency and participation of parties. Thus, this depicts that trust value is multidimensional and cannot be measured by single source.

Context-dependent. Trust is related to overall contexts and may vary for different targets. Social context may influence trust evaluation; consequently, trust value should be considered as a function of information context.

It can be deduce that trust features are mutually correlated. It is noted that transitivity is related to the context or multidimensionality can affect transitivity. Considering all features of trust to compute its value required complicated computation and it is out of scope of this study. In this study, we attempt to focus further on transitivity, as our main goal is to measured trust value in information propagation; thus, transitivity feature of trust is required as trust can be transitive under positive semantic restrictions and not always in real life. The ability to refer to a third party let trust to be transit and it is known as referral trust.

B. *Related works*

Trust has a complex meaning and its calculation is not easy [7]. There are many trust inference algorithms that can be used in social network sites. All of these algorithms are based on trust transitivity. We mention some related works that have been done on trust in computer science and social interactions as follows. Yu and Singh proposed a model that builds a social network among users which supports participants' reputation. Each user has other users in his/her list and measured the trustworthiness of other users according to the gained values from reliable referral chains. When one user gains bad experience, the result will disseminate through network and consequently others can update their list ratings [20].

Abdul-Rahman and Hailes describe a model in which trust can be measured based on observed reputations [21]. Kamvar et al. used the Eigen Trust algorithm in peer-to-peer systems and calculate trust with a variation on the PageRank

algorithm that is used by Google to rate the relevance of web pages to a search. A matrix of trust values that are worldwide accepted by peers is used by algorithm and the result depicts that the EigenTrust is resistant to attacks [22].

Jøsang et al proposed a method for trust network analysis based on graph simplification and trust derivation with subjective logic that is called Trust Network Analysis with Subjective Logic (TNA-SL). Although TNA-SL can detect and disseminate negative trust rapidly, it needs to be simplified multipart and complicated networks that may cause information loss [23]. The probabilistic explanation for confidence in social networks was explained by Kuter and Golbeck. They use Sunny, an inference trust algorithm to measure confidence and trust [24].

Vydiswaran et al presented a content-driven trust computation framework to calculate the trustworthiness of sources by joining the quality of evidence content. This framework forms trustworthiness in unstructured domain and increase the possibility of finding trustworthy sources [25]. All these related works, graph-based approaches, logic-based approaches and probabilistic models are for analyzing trust. In this paper, we propose new algorithm to evaluate trust level in information diffusion. We consider strong ties and weak ties in a social graph in order to explore the role of trust in dissemination of information throughout a social network site.

V. TRUST MODEL DEVELOPMENTS

Trust is impacted by various types of factors such as trustor, trustee, relationship and the context between these two participants [26].Trust can be transitive under positive semantic restrictions and not always in real life. The ability to refer to a third party let trust to be transit which is known as referral trust. The length of the trust target has direct relation with the length of the transitive path. Trust transitivity can be influenced by the recommendation roles of the participants, different domains and also the participants' relationships [27].

Trust models can be categorized as in Table 1; based on the trust transitivity strategies. Each strategy has its own method for calculating the trustworthiness of a target participant. In Multiplication strategy, trustworthiness value can be calculated by the multiplication of the trust values between any two participants. In Averaging strategy, trustworthiness value can be computed based on averaging the trust values between any two participants; and it can be calculated based on the confidence of a target participant on the trust value of any two participants in confidence-based strategy.

Table I. Trust transitivity strategy and calculated trustworthiness

Types of Strategy	Calculated Trustworthiness	Source
Multiplication strategy	1. If participant A trusts participant B with trust value $T_{(AB)}$ 2. If participant Btrusts participant C withtrust value $T_{(BC)}$ 3.If $T_{(AB)}, T_{(BC)} \in [0, 1]$ (1.2.3) ➡ $T_{(AC)} = T_{(AB)} * T_{(BC)}$	•Walter, Battiston, and Schweitzer (2008) • Li, Wang, and Lim (2009)
Averaging strategy	• $T_{(Ac)}$= (Wi * $T_{(AB)}$ + Wj* $T_{(BC)}$)/ 2 • Wi+ Wj= 1	• Gray et al. (2003) •Golbeck and Hen dler (2006)
Confidence-based strategy	• Basedon $T_{(AB)}$, $T_{(BC)}$ • Confidence of person A on $T_{(BC)}$(CA) • CAis calculated based on the similarity between person A and person B	•Guha et al. (2004) •Kuter and Golbeck (2007)

VI. EVALUATION OF TRUST VALUE IN INFORMATION DIFFUSION

A social network is the specific type of a network that can be defined as a set of users interconnected via relationships. A node represents a participant (user) and links between nodes represent online interactions among them. Participants are connected via their social activities which can be defined as a social interaction. Social activities of a participant and his/her friends can be used to calculate trust value according their interactions. A calculated trust value can be used to compute amount of information dissemination through a social network.

We consider a social network as graph G (N,E) according to the graph theory in order to calculate i) trust value and, ii) amount of information dissemination. N indicates nodes (participants) and E indicates edges (relationships). We divided the graph into clusters that each cluster contains strong ties and weak ties. A cluster sample of graph is depicted as follows. The nodes inside the cloud are strong ties and the nodes which are outside the cloud are weak ties. Gray nodes are active ties.

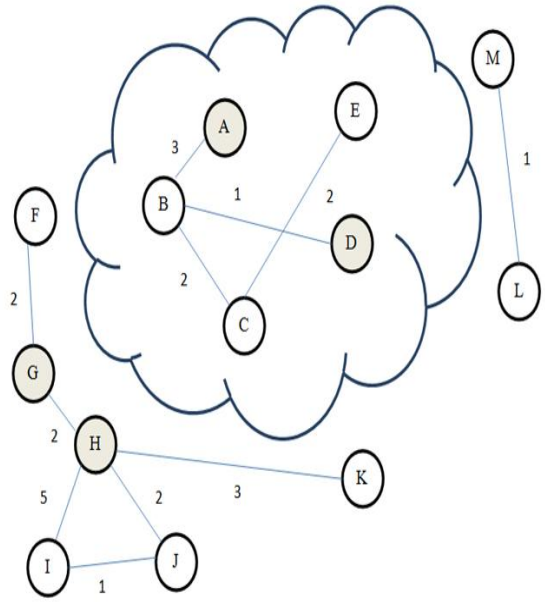

Fig I. Sample of a Social Network

$T(U_x, U_y) \in [0, 1]$ denotes trust value that U_x allocates to U_y. If $T(U_x, U_y) = 0$ indicates that U_x completely distrusts U_y and if $T(U_x, U_y) = 1$ indicates U_x completely trusts U_y for future action. U_x or U_y indicates any participant (user) in a social network. Trust value can be computed between two nonadjacent participants if there is a trust path linking them; in other word, another participant who has relation with two nonadjacent participants (U_i) can be used in order to calculate trust value. This is based on the transitivity feature of trust.

$$N = \{N_{U_t} \mid U_x < U_i < U_y\} \quad (1)$$

N indicates the number of nodes (participants) between two nonadjacent participants. Therefore, trust value between participants can be computed according to the Formula (2) as follows.

$$T(U_x, U_y) = \frac{1}{D(U_x, U_y)} \sum \frac{(N * \sum N(U_x U_y))}{\sum_{i=1}^{n} N_i} \quad (2)$$

$D(U_x, U_y)$ is the length of a shortest path between U_x and U_y. N_i indicates the number of total interactions in a graph.

The amount of trust value can be used to calculate the probability of information propagation throughout a social network. The likelihood of information diffusion varies among of strong and weak ties [28]. And it can be calculated based on the formula (3) as follows.

$$IS(U_x, U_y) = \frac{\sum N(S|A) + N(W|A))}{\sum N} * T(U_x, U_y) \quad (3)$$

$IS(U_x, U_y)$ indicates the chance of information sharing that can be calculated by dividing the number of active strong or active weak ties by the total number of the strong or weak ties by multiplication with trust. Table 2 delineates results based on the Fig (I) and formulas (1, 2, 3).

Table II.Trust value and likelihood of information propagation among ties

Participants	Distance	Trust	Likelihood of Information Propagation
$N_{(S,S)}: N_{(A,C)}$	2	0.31	0.12
$N_{(W,W)}: N_{(F,H)}$	2	0.13	0.04
$N_{(S,S)}: N_{(A,E)}$	3	0.58	0.23
$N_{(W,W)}: N_{(F,I)}$	3	0.4	0.13
$N_{(S,W)}: N_{(A,C)}$	2	0.08	0.02
$N_{(S,W)}: N_{(A,F)}$	3	0.16	0.05

The results depict that trust has direct effect on information propagation. It also illustrates that trust among strong ties are more than trust among weak ties. Additionally, it is proven that trust between one strong tie and one weak tie will result in less than two of the same ties.

VII. CONCLUSION AND FUTURE WORK

This study had successfully identified the role of trust in information propagation throughout social network sites by strong ties and weak ties. The proposed algorithm formulates the amount of trust value in information dissemination. It depicts that trust is an important element for all online transactions which plays a significant role in social relations by blocking the distrust transitivity and decrease the sophistication of trust path. In SNSs, trust affects the users' decision in dissemination of information. Consequently, it can provide both positive and negative sense of security. Although calculation of trust value cannot be completely accurate; but providing trustworthy online social network sites is as significant as the concept of these sites are sharing information. Thus, in this paper, we review trust features, models and roles in online social network sites, with some previous works regarding to measuring the trust value in information propagation. We propose an algorithm that computes trust value in information propagation. Providing a trust-worthy online social network site that preserve users' trust and privacy through information disclosure is a subject of our future work.

ACKNOWLEDGEMENT

The authors would like to thank Ministry of Education, Government of Malaysia and Research Management Centre, Universiti Teknologi Malaysia for supporting this research with grant number 4F237.

REFERENCES

[1] R. Gross, "Information Revelation and Privacy in Online Social Networks," The 2005 ACM Workshop on Privacy in the Electronic Society, 2005, pp.71-80.
[2] C. Lampe, N. Ellison, and C. Steinfield, "A Face (book) in the crowd Social searching vs.social browsing,"The ACM Special Interest

Groupon Computer- Supported Cooperative Work, Banff, Canada, 2006.
[3] D. Fono, and K. Rayes-Goldie, "Hyperfriendship and beyond: Friends and social norms onLiveJournal,"Internet Research Annual, vol. 4, 2006, pp. 91-103.
[4] Y. Wang, and M.P. Singh, "Trust representation and aggregation in distributed agent system," In: Proceedings of the 21st National Conference on Artificial Intelligence (AAAI). Boston, MA, USA,2006, pp. 1425–1430.
[5] A. Jøsang, S. Pope, and M. Daniel, " Conditional deduction under uncertainty," in Proceedings of the 8th European Conference on Symbolic and Quantitative Approaches to Reasoning with Uncertainty (ECSQARU 2005), 2005.
[6] J. Riegelsberger, A.M. Sasse, andJ.D. McCarthy, " The mechanics of trust: A framework for research and design,"International Journal of Human-Computer Studies, 2005, pp. 381–422.
[7] L. Mui, M.Mohtashemi, and A. Halberstadt , "A Computational Model of Trust and Reputation," Proc. 34th Hawaii International Conference on System Sciences, 2002.
[8] J. Golbeck, and J. Hendler, " Inferring binary trust rela-tionships in Web-based social networks,"ACMTrans. Internet Technol, 6(4), 2006,pp.497-529.
[9] D. Boyd, "Friendster and publicity articulated social networking," In Conference on Human Factors and Computing Systems (CHI 2004), April 24-29, Vienna, Austria, 2004.
[10] G. S. Mesch, and I.Talmud,"Online Friend-ship Formation, Communication Channels, and Social Closeness," International Journal of Internet Science, 1 (1), 2006, pp. 29- 44.
[11]]N. Coppola, S.R.Hiltz, and N. Rotter, "Building Trust in Virtual Teams," IEEE Transactions on Professional Communication (47) 2, 2004, pp. 95-104.
[12] V. Buskens, "Social networks and trust," in The Nether-lands: Kluwer Academic Publishers, 2002.
[13] M. Siegrist, and G. Cvetkovich, "Perception of Hazards: The Role of Social Trust and Knowledge. Risk Analysis, 20(5), 2000, pp.713-719.
[14] M.J. Metzger," Effects of site, vendor, and consumer characteristics on Web site Trust and disclosure. Communication Research, 33, 2006, pp.155–179.
[15] C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern withinsocial networking sites: A comparison of Facebook and MySpace", Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado, 2007.
[16] J. Ahn, "Teenagers and social network sites: Do off-line inequalitiespredict their online social networks", peer-reviewed journal on the internet,vol.17, Number 1-2 January 2012.
[17] C. Lampe, N. Ellison, and C.Steinfield, "A Face (book) in the crowd: Social searching versus social browsing." Proceedings of the 20th Anniversary Conference on Computer Supported Cooperative Work, Banff, Alberta, Canada, 2007.
[18] J. Golbeck, and J. Hendler, " Inferring binary trust relationships in Web-based social networks,"ACM Trans. Internet Technol., 6(4), 2006, pp.497-529.
[19] P.D. Meo, et al., " Finding reliable users and social networks in a social internet -working system," In Proceedings of the International Database Engineering & Applications Symposium, Cetraro- Calabria, Italy: ACM, 2009, pp. 173-181.
[20] Y. Bin, and M. P. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," Proc. of the 4th International Workshop on Cooperative Information Agents, Matthias Klusch, Larry Kerschberg (Eds.), Lecture Notes in Computer Science, vol. 1860, Springer, 2000.
[21] A. Abdul-Rahman, ans S. Hailes, "Supporting trust in virtual communities," in Proceedings of the 33rd Hawaii International Conference on System Sciences, 2000.
[22] S. Kamvar, M.Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," In International Conference on World Wide Web (WWW), 2003.
[23] A. Jøsang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," In Australasian Computer Science Conference (ACSC), 2006.
[24] U. Kuter, and J. Golbeck, "Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models," in AAAI, 2007, pp. 1377–1382.
[25] V. Vydiswaran, C. Zhai, and D. Roth, "Content-driven trust propagation framework,"In Knowledge Discovery and Data Mining (KDD), 2011, pp. 974–982.
[26] D.Z. Levin, and R. Cross, "The strength of weak ties you can trust: The mediating role of trust in effective knowledge transfer," Management Science, 50(11), 2004, pp.1477–1490.
[27]]R. Miller, D. Perlman, and S. Brehm, "Intimate Relationships,"McGraw-Hill College, 4th edition, 2007.
[28] S. Kavianpour ,Z. Ismail, and BH. Shanmugam, "Differences between Role of Strong Ties and Weak Ties in Information Diffusion on Social Network Sites,"Book Chapter of Advanced Research and Trends in New Technologies, Software, Human-Computer Interaction, and Communicability, August 2013.

Sanaz Kavianpour studied master of computer science (information security) at the Advanced Informatics School, Universiti Teknologi of Malaysia International Campus Kuala Lumpur. She has published about 8 papers in local and international conferences, journal and book in the fields of social networking, information diffusion, anonymity and algorithms.

Dr. Bharanidharan Shanmugam, is a Researcher/Senior Lecturer/Consultant at Advanced Informatics School, Department of Information Security, Universiti Teknologi Malaysia (UTM). He holds Doctorate degree in computer science specializing in network security from UTM. He has vast experience in mentoring and his research area is focusing more into ethical hacking and its countermeasures.

Dr. Zuraini Ismail is an Assoc. Prof at UTM advanced Informatics School, Universiti Teknologi Malaysia International Campus Kuala Lumpur. Her research interest lies in Information Security Management Systems , Information Security Policy, Information Security - Awareness and Ethics, Information System Management Security, Cyber Security, Knowledge Management, e-Government and IT Outsourcing.