Advance on Trust Model and Evaluation Method in Social Networks

Lijun Yang, Zhiyong Zhang, Weili Tian, Qingli Chen
Electronic Information Engineering College
Henan University of Science & Technology
Luoyang, China
e-mail: z.zhang@ieee.org

***Abstract*—With the rapid development of electronics, communication networks and information technologies, there are emerging more and more open Internet-based web services and versatile applications. Users or agent entities accomplish their effective interactions and transactions based on the essential trust relations, and the trust assessment would provide secure services, privacy protection and trustworthy decision and for large-scale complicated networks. The basic attributes and represents of trust are firstly presented, and then the trust assessment theories and algorithms are classified and analyzed. The state-of-the-art of trust management, including the trust model, transmission and measure, are detailed discussed in the emerging social networks with small-world feature. Finally, some open issues and challenges of trust assessment are highlighted, in combination with a novel research direction of trust modeling on digital contents share and distribution in multimedia social network.**

Keywords-Open Networks; Trust assessment; Algorithm; Social network; Small-world theory

I. INTRODUCTION

With the rapid development of network information technology, the Web-based application mode has changed from centralization to distribution. The distributed network has demonstrated its obvious advantages in terms of coordinated work, sharing of distributed information and resources, and large-scale parallel computation, among others. At present, it has become the direction for development of modern network applications and services. Consequently, trust management and trust assessment have become the foundation for data interaction, content transaction, and inter-operation among entities; they have also allowed managers to make reliable decisions.

As a generic natural attribute present in human society, "trust" is usually understood as a concept of subjective intuition without a uniform definition. In sociology, trust is usually defined as the reliable dependence on people or the features of things, capacities, power, or honesty. In the information technology sector, Marsh first discussed the concept of trust in 1994. In that work, the author divided the content and degree of trust and presented the mathematical model of trust measurement in light of the subjectivity of trust, thus laying the foundation for the application of trust in computer science [1]. Subsequently, Blaze [2] and other researchers presented the concept of trust management, with the aim of solving security problems involving Internet services. The basic idea is to admit that security information in an open system lacks integrity, and that the security decision-making of a system requires security information provided by a trustworthy third party. They also presented the idea of a security decision-making framework, which is relevant to the distribution of Web application systems and their dynamic features.

In view of the application of trust relationship in an open network system, Gambetta [3] redefined trust as a measurement of subjective probability level, in which one entity performs a particular behavior in a certain time and certain contextual conditions against another entity. This concept presents a trust degree measurement of the target object before an undetermined behavior occurs. Thus, by measuring and assessing the potential trust information between entities in various network environments, the trust mode supplies the Web system with a relatively flexible management mechanism and security measurement method [4].

II. EVALUATION OF SOCIAL NETWORK TRUST

A. Social networks and the small world theory

A social network is a typical application of the small world network theory based on trust relationships among people in society [5]. It provides a platform, through which users can maintain their social relationship networks. Users in the same network can exchange and share information and boost interactions with a series of well-defined functions.

The small world theory is also called the 6-degree of separation theory, which describes a highly interesting phenomenon, i.e., there is a maximum of 6-degree separation between an individual and anyone else on the planet. Watts and Strogatz [6] described the small world network with pictures, indicating that such a network is one between the regular network and the random network. The small world network has two remarkable features, namely, a large concentration ratio and a short average path length. A large concentration ratio means that the nodes in the network are relatively closely connected, whereas a short average path length means that any two nodes in the network can be connected by a shorter path. The small world network theory has been widely studied due to its remarkable features. Many networks in real life can be considered small world networks, such as the electricity supply network, relationship networks among actors and actresses, the nerve networks of worms, and the increasingly popular social networks.

978-0-7695-4763-3 2012

DOI 10.1109/ICGEC.2012.41

At present, many social networks, such as MySpace and Facebook, have been created via the Internet. Among these networks, the identities of many entities are unknown in real life; such entities may not even have any previous direct connections with one another. To a certain extent, social networks reflect the network structures of an actual society and assemble a significant amount of real information within the networks. Moreover, some vicious users establish reliable relationships with normal users to collect their private information and send out junk advertisements. Social networks currently face a variety of security concerns, such as phishing [7], theft of commercial data, rubbish messages distribution, data bank engineering reversions, and so on [8].

In reality, we are prone to talking to people whom we trust; furthermore, we also tend to believe those who are recommended by people we know well. In this sense, the social relation network is regarded as a small world network. Similarly, we can impose limits on relevant safety operations according to the trust relationships of nodes in a computer network environment.

Considering that the social network is established based on trust relationships, it contains rich trust-relevant information that can be used to infer and evaluate the trust relationships among participating users and entities. Furthermore, the degree of trust inferred provides instruction to many applications, such as recommending products to people whom we trust, or recruiting reliable employees in the social networks. Limits on visitors and information publication can also be set, in accordance with the trust relationships to prevent and minimize various kinds of safety risks in social networks.

B. Model of trust network

Based on the small world network theory, Venkatraman [9] regarded a file or information sharing network as a social network and stated that among sub-communities, pivot nodes (i.e., those connecting different sub-communities) have weak connections. In a small world, boundary nodes between different domains have a relatively low concentration coefficient within each domain, although they are responsible for connecting different domains. Furthermore, other nodes within the same domain have a greater chance to acquire a huge amount of information on other domains when they are connected to the nodes with a weak connection relationship. Moreover, Venkatraman [9] revealed that the existence of these pivot nodes can improve the quality of the network.

Enlightened by the small world theory and real social relationship networks, Guo et al. [10] stated that the establishment of a trust network in an open network environment can provide a strong basis for the security of a real network environment. The authors reported that a social network has two typical features, namely, the small world feature and the scale-free feature. The small world feature refers to the fact that a network has a large concentration coefficient and a shorter average path length. A shorter path can always be found to connect any two nodes in a network. This is also an expected attribute of a trust network. The most distinct feature of a scale-free network is that the degree distribution of nodes in the network is subject to the power laws. This is because the degree distribution of some nodes is far beyond the average value.

Although some models have been presented to explain the small world and the scale-free features, no model has yet to explain both. Based on the research on the small world model and the scale-free network model, Guo et al. proposed a method of constructing a trust network incorporating both the small world and the scale-free feature in an attempt to create an overall trust network to act as a part of the security infrastructure. However, this process of building a small world trust network is not specific.

Based on the work of Guo et al. [10], Zheng et al. [11] revealed that, in order to reduce resources necessary for maintaining the trust network, each node only has to maintain one list containing a direct trust relationship during the trust network construction process. They also reported that the trust network must have the capacity to find a recommendable short trust path between any two nodes quickly. Thus, they proposed the idea of small world construction; in this proposal, a sparse trust network is first constructed due to the fact that the degree distribution of the nodes must comply with the power laws so that the sparse trust network can greatly reduce expenses. Then, two principles are followed, namely, the priority of partial trust network and the addition of a necessary long-distance shortcut. Figure 1 illustrates the two principles and shows that there is a lesser trust relationship existing between nodes that are far away from each other. Although their idea of constructing a small world trust network is relatively insightful, the method proposed by Zheng et al. [11] is not well justified.

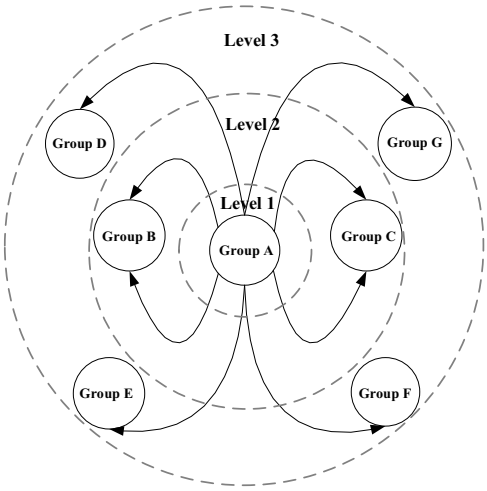

Figure 1. Principle for adding long-distance shortcut [11]

Meanwhile, James et al. [12] presented the SocialTrust, a trust construction framework with modification elasticity in online social networks. SocialTrust distinguishes relationship from trust and has an individual feedback system, which adapts to changes of the social networks and modifies trust in a dynamic way.

However, it is almost impossible to yield reliable trust results using the traditional trust inference system based on a simple trust network. To address this, Liu et al. [13] constructed a complicated trust-oriented social network structure, which combines trust value, social relationship, and recommended roles; their proposed structure presents the trust inference mechanism in combination with the Bayesian network. Although their concept of trust inference mechanism has been proven to be imperfect, it has good performance in complicated trust-oriented social networks. Nevertheless, constructing a complicated trust-oriented social trust network is necessary.

Kang et al. [14] used a socialized network dynamic model for the emerging social networks to simulate the self-organization process of the socialized network structure. They also analyzed the characteristics of the vicious nodes by constructing their own trust networks and making vicious trust expansion. They reported that vicious nodes have a greater chance of increasing the connection level, usually constructing their trust networks with the minimum concentration coefficient strategy. Thus, to distinguish normal users from vicious users, Kang et al. [14] presented three trust evaluation methods: those based on the connection, self-trust and the mutual trust levels, respectively. Furthermore, they also presented trust control and reduction strategy based on the above. The mutual trust level method can be used to screen vicious nodes with utmost precision according to their own characteristics. Subsequently, the trust control and reduction strategy can be used to inhibit vicious nodes. However, a special case may occur, i.e., vicious users can counterbalance the risks from service terminals and other users by controlling their own concentration coefficients to minimize overall risks. This case has not been well addressed; nevertheless, the simulation of the trust network organization and construction process proposed by Kang et al. [14] is relatively referential and helpful.

C. Trust relationship description and trust transfer

The growth and the small world nature of social Web-based networks offer great potential for the application of intelligent software, which combines social networks and personal preferences. How can trust information be explored in Web-based social networks and how can such information be integrated into the trust evaluation of social networks? These are the main issues addressed in social network applications. To find solutions, many scholars have conducted extensive research on trust relationship description and trust transfer, and attempted to apply trust mechanisms in social networks by describing the trust relationships in social networks and designing trust inference algorithms to discover the rules for the transfer of trust relationships.

Jennifer et al. [15] described the trust relationship in a Web-based social network as follows: trust is a kind of belief and a kind of guarantee, and the entity's behavior in the future can elicit results as good as expected. The authors used {0, 1} to represent trust relationship, in which 0 stands for distrust and 1 stands for trust. Trust is indicated to have transferability, asymmetry and subjectivity, and the influences these attributes have over information inference are discussed. Based on individual opinions and the recommendation rating information of other entities in a trust network, two information inference algorithms (i.e, Rounding and Nonrounding) have been presented to rate individuals without direct connection in a network and infer trust relationships. The two algorithms differ slightly in synthesizing different recommendation path trust inferences: the former rounds the satisfaction proportion of the rating information, whereas the latter creates averages. Suppose the final trust inference form meets formula (1), then it is a highly precise trust inference given by:

$$\lim_{n\to\infty}\sum_{i=\lceil n/2\rceil}^{n}\binom{n}{i}a^{i}(1-a)^{n-i}\to 1 \quad for \;\; a>0.5 \qquad (1)$$

where n represents the number of nodes in the trust network formed between the source entity and the target entity; i is the number of positively rated nodes in the trust network; and a is the parameter for the basic evaluation precision in the network. Jennifer et al. [15] compared the two calculations using theoretical analysis and simulation experiments, as well as the initial node trust level in the network formation process. The results demonstrate the precisions of the two trust inference proposals. Based on these results, they designed an e-mail client terminal called, TrustMail, to make ratings according to the reliability level of the e-mails in the inboxes of the users.

The research of Jennifer et al. [15] focused on trust inference, in which they adopted the two-value method to describe trust relationship. Compared with the continuous trust value expression method, this method is unable to explain the complexity of trust and the precise trust relationship between users. Moreover, the trust inference algorithm fails to consider the characteristics of the network topological structure, but only distributes uniform value to benign nodes. However, nodes closer to the source node actually have a greater tendency to be trusted compared with nodes that are far away from the source node. This means that a better result can be achieved if limits on the length of the recommended path are defined between the source node and the target node.

Contrary to the work of Jennifer et al. [15], Javed et al. [16] considered publication networks as examples and used relational algebra to express and infer trust relationships widely existing in social networks comprising different elements and entities belonging to different combinations in terms of their nature. The authors divided publication networks into five combinations, namely, author, thesis, periodic and reviewer, and described the relationships among members of the networks using a relational matrix. Suppose A represents the vector of the author member combination, and P stands for the vector of the typical thesis member combination, we then obtain $Mr = A \times P$ which is the relational matrix from author to thesis. In this matrix, the size of each element m_{ij} stands for the strength of the relationship. With regards the operations of the relational

matrix, such as crossing, eliminating diagonal elements and combining, Javed et al. [16] defined a series of semantic operators, such as value equivalence, fusion, reversal, semantic switch, and so on, to express, track, infer, and analyze all kinds of complicated social relationships and their mutual influences. Afterwards, the authors applied them to the selection of thesis reviewers and columns in the publication network.

Moreover, Javed et al. [16] thought that computations in social networks are different from those in a relationship database. Such computations require true and important calculations, such as the dissipation strength of trust relationship and the operation of relationship matrix with relational algebra to infer trust relationships potentially existing in social networks. This allows the localization of trust relationships and the proper dissipation of relationship strength. The authors also imagined its broad application prospect and confirmed commentators in nonprofessional networks of conference management systems. They also discovered intellectual property right concerns in the publication system and sought individuals with stronger immunity to infectious diseases as well as the application of social network in crime prevention. Finally, Javed et al. [16] emphasized that privacy protection is expected to become an increasingly important issue due to the rapid development of social network applications. Moreover, they also reported that multi-value logic is suitable for trust calculation in complicated social networks. Anna [17] presented a trust model based on the intuitionistic fuzzy set (IFS) theory. The author conducted research on trust modeling and transmission in trust network, and used relevant IFS base cardinalities to measure trust transmission. This model is appropriate for large-scale networks, although the t-norm and cardinality patterns used in the model are quite monotonous. Furthermore, the maximum transmission path length of trust is undefined, resulting in its failure to explain networks of smaller sizes.

In recent years, the social information system has become a promising new model in large-scale information management. This is proven by the rise of large-scale information-sharing communities, social media Websites, and Web-based social networks. As individual users and their computers are becoming increasingly dependent on these social systems, they become more exposed to greater risks. These social systems give more opportunities to vicious participants to exploit the close-knit organizational structure of these networks. To tackle these problems, James et al. [12, 18] presented the SocialTrust framework to ensure the management of trustworthy information in social information systems under current Internet conditions. The authors analyzed numerous inherent flaws of online social networks and introduced the SocialTrust framework to establish trust relationship description with a certain level of modification elasticity. They utilized feedbacks from trust groups to differentiate relationship quality and trust among users as well as to monitor trust transmission among users. They presented the principal trust inference method to provide trust opinions to users based on social network dimensions. The authors then created an individualized extension of SocialTrust and presented the idea of mySocialTrust. Furthermore, they conducted experiments using millions of MySpace user files and social network data sets of user relationships, consequently proving that mySocialTrust can offer a user-centered optimal trust idea. Compared with other trust descriptions or trust inference algorithms, mySocialTrust considers those important factors that affect trust structure, thus commanding the feature of large-scale experimental evaluation. Moreover, even if large-scale vicious group coordination exists, SocialTrust is also able to support stable trust construction. Nonetheless, SocialTrust needs to be expanded in terms of its contextual scenario so as to support additional expressions of trust opinions.

D. Trust measurement and evaluation

With the discovery of the shortcomings and disadvantages of social networks, high-end and popular applications, such as Web-based social networks (WBSNs), have emerged in recent years. With the increased likelihood of vicious behaviors occurring in WBSNs, evaluating the trustworthiness level of individual has become a necessary condition prior to communication. Therefore, it is important to identify the trust degree of one individual over another within the network. One method to do so is to use the trust measurement or trust evaluation.

Muthucumaru et al. [19] revealed that an important problem existing in Web-based social networks is trust management. In their work, they focused mainly on trust modeling in social networks and presented the gravity-based model for trust evaluation. The authors used the distributed virtual coordinate system to distribute virtual coordinates in order to quantify trust and administer activities within social networks. However, their model can only be used to quantify trust relationships within the surrounding areas of the nodes; moreover, the trust measurement algorithm only considers the distances between nodes and thus has great limitation.

Interestingly, based on the concept of resistive network, Mohsen et al. [20] presented a new trust inference model, which they call RN-Trust. In this model, the trust network is expressed by a resistive circuit, and each trust relationship is reflected as an ideal combination of diodes and resistors. A diode is used to express the asymmetry of trust in real world; a resistance value is used to reflect the strength of the trust relationship; and a logarithmic function is used to map the resistance value into the trust value. However, in the real world, the magnitude of social networks is huge, making it difficult to use resistive circuits to express the structure of social networks.

Zhai et al. [21] conducted research on current social network theories and trust models and presented an e-commerce trust model based on a social network. In this model, as a node's self-trust value increases, the inter-node trust path shortens accordingly when the node enters the small circle of the initial node. They also presented an algorithm to seek the trust recommendation path, while considering such factors as the importance of network members, the trustworthiness level of recommended nodes, the time attenuation of trust value, and money-related

transaction risks, among others. Their simulation results show that the social network-based trust mechanism can identify and eliminate false nodes in real time and withstand trust attack activities in the network. The model presented by Zhai et al. [21] provides a reliable environment, in which to safely conduct e-commerce transactions among network members. However, the trust and coordination combination mode of the model is not flexible enough and cannot effectively eliminate intentional trust attacks.

In recent years, social media such as blogs, social networks, micro-blogs and user comment Web sites have gained increasing popularity. Thus, social network analysis has been receiving increased attention as well among researcher. These media units typically serve as platforms for information transmission, embedded advertisements, or commodity promotion. In this general environment, influence and trust level have become the fundamental features that users consider when they interact with one another. Varlamis [22] conducted extensive research on multiple measurement standards related to these elements. Presenting an individualized trust model, the author also studied the features of information transmission in the virtual world. First, the model distinguishes permanent connection from temporary connection and considers the latter's freshness to better understand the connection attributes and the dynamism of the social network. Varlamis [22] reported that the roles in social networks might be those of users, blogs or SMS, and considered the trust opinions of one role over the others, the trust opinions of role trust networks, the comprehensive ratings of all roles, as well as the locations and mutual relationships of roles in the trust pictures. The author distinguished partial influence from overall influence to infer trust relationship. By contrasting recommendations provided by partial trusted users and those provided by overall trusted users, the model recommends similar or influential roles in a social network to particular users. However, given that the algorithm presented by Varlamis [22] simultaneously considers partial trust and overall trust, the algorithm may become overly complicated and unrealistic when applied to a large-scale network.

More importantly, Yuan et al. [23, 24] revealed in the documents that the trust network is formed based on the inter-node trust relationship and is generally regarded as a small world network. Few researchers have examined the assumption that the trust network is a small world network due to the dynamism of the trust network. Yuan et al. [23] presented the traditional way of examining the small world feature; here, if a trust network has a relatively large concentration coefficient and a shorter path length, it is indicated to be a small world network. Yuan et al. [24] concluded that considering the dynamic changes in the trust network, and the fact that the proposed method only adopts static data at a particular time point, it can only offer limited proof that the trust network has the small world feature at that particular time point; moreover, this is insufficient in proving that the dynamic trust network is a small world network. Hence, some researchers presented a new examination method. First, they presented proof stating that the degree distribution of nodes in the five trust networks solicited online complies with the power laws and that the network is a scale-free network. They have also proven that thte topological structure of the scale-free network is independent from the dynamic changes of the network, which is a good demonstration of the fact that a dynamically changing trust network is a scale-free network. As such, it is a small world network, which in turn, proves that the scale-free network is a kind of small world network. The researchers used the small world network feature to improve the traditional trust apprehension recommendation system (TARS). The final trust value synthesis of the traditional TARS trust evaluation algorithm is shown in formula (2):

$$p_{a,i} = \overline{r_a} + \frac{\sum_{u=1}^{k} w_{a,u}(r_{u,i} - \overline{r_u})}{\sum_{u=1}^{k} w_{a,u}} \qquad (2)$$

The predicted evaluation of activity user a in aspect; No. i is the average value of the evaluation in all aspects (it is also the average value of the evaluation of the recommended user u in all aspects and the recommended information of u in aspect); and k is the number of effective recommendations. The weight of activity user a to recommender u is shown in formula (3). Here, MTPD is the trust dissipation distance between a and u:

$$w_{a,u} = \frac{d_{\max} - d_{a,u} + 1}{d_{\max}} \qquad (3)$$

MTPD is the maximum effective recommended path length and is the most important parameter in TARS; however, the traditional TARS model is unable to provide the appropriate value. Yuan et al. [24] maximized the property, which states that the small world network has a relatively average path length, and suggested using the average path length of the trust network as the value of MTPD. They have also conducted simulation experiments, proving that the improved TARS model has the maximum trust predication precision and a relatively smaller time complexity. However, they did not make specific optimizations of the algorithms in the TARS prediction evaluation mechanism.

III. SUMMARY

Thus far, trust has become the key technology of Internet-based e-commerce, distributed applications, and system safety. Moreover, as the Internet expands in scale and new network application technologies grow rapidly along with it, trust is expected to play an increasingly important role and have great application potential. However, as exemplified by the studies explained above, relevant trust evaluation technologies are still in the initial phase of development.

ACKNOWLEDGMENT

The work was sponsored by National Natural Science Foundation of China Grant No.61003234, Program for Science & Technology Innovation Talents in Universities of Henan Province Grant No.2011HASTIT015.

REFERENCES

[1] S. P. Marsh. Formalizing Trust as a Computational Concept, UK: University of Stirling, 1994.

[2] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," Proc. of the 17th Symposium on Security and Privacy, IEEE Press, May.1996, pp.164-173, doi:10.1109/SECPRI.1996.502679.

[3] D. Gambetta, Can We Trust Trust? Trust: Making and Breaking Cooperative Relations, UK: University of Oxford, 2000, pp.213-237.

[4] L. Rasmusson and S. Jansson, "Simulated social control for secure internet commerce," Proc.of the 1996 ACM Workshop on New Security Paradigms, ACM Press, 1996, pp. 18-25, doi:10.1145/304851.304857.

[5] L. Sorensen, "User managed trust in Social Networking-comparing Facebook, MySpace and Linkedin," Proc.of the 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, IEEE Press, May. 2009, pp.427-431, doi:10.1109/ WIRELESSVITAE.2009.5172486.

[6] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," Nature, vol.393, June.1998, pp.440-442, doi:10.1038/30918.

[7] D. Rosenblum,"What anyone can know: The privacy risks of social networking sites," IEEE Security and Privacy, vol.5, June.2007, pp.40-49, doi:10.1109/MSP.2007.75.

[8] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective Privacy Management in Social Networks," Proc. of the 18th international conference on World Wide Web, ACM Press, 2009, pp.521-530, doi:10.1145/1526709.1526780.

[9] M. Venkatraman, B. Yu, and M. P. Singh, "Trust and Reputation Management in a Small-World Network," Proc. of Fourth International Conference on Multi-Agent Systems, IEEE Press, Jul.2000, pp.449-450, doi:10.1109/ICMAS.2000.858519.

[10] X. Guo, X. Li, Y. Qin, and C. Chen, "Modeling Small-world Trust Networks," Proc. of the 2008 International Symposium on Ubiquitous Multimedia Computing, IEEE Press, Oct.2008, pp.154-159, doi: 10.1109/UMC.2008.38.

[11] J. Zheng, Y. Qin, and J. Zhu, "Constructing Trust Networks Based on Small-World Theories," Proc. of the 9th International Conference for Young Computer Scientists, IEEE Press, Nov.2008, pp.1957-1962, doi: 10.1109/ICYCS.2008.469.

[12] J. Caverlee, L. Liu, and S. Webb, "Towards Robust Trust Establishment in Web-Based Social Networks with SocialTrust," Proc. of the 17th International Conference on World Wide Web, IEEE Press, 2008, pp.1163-1164, doi: 10.1145/1367497.1367707.

[13] G. Liu, Y. Wang, and M. Orgun, "Trust Inference in Complex Trust-oriented Social Networks," Proc. of the 12th IEEE International Conference on Computational Science and Engineering, IEEE Press, Aug.2009, pp.996-1001, doi: 10.1109/CSE.2009.248.

[14] L. Kang, J. Jing, and Y. Wang, "The Trust Expansion and Control in Social Network Service," Journal of Computer Research and Development, vol. 47, Sep.2010, pp.1611-1621.

[15] J Golbeck, and J. Hendler, "Inferring Binary Trust Relationships in Web-Based Social Networks," ACM Transactions on Internet Technology, vol.6, Nov.2006, pp.497-529, doi:10.1145/1183463.1183470.

[16] J. I. Khan, and S. S. Shaikh., "Computing in Social Networks with Relationship Algebra," Journal of Network and Computer Applications. vol.31, Nov.2008, pp.862-878, doi:10.1016/j.jnca.2007.04.004.

[17] A. Stachowiak, "Trust Propagation-Cardinality-Based Approach," Proc. of the International Multiconference on Computer Science and Information Technology, IEEE Press, Oct.2009, pp.125-129, doi: 10.1109/IMCSIT.2009.5352807.

[18] J. Caverlee, L. Liu, and S. Webb, "The SocialTrust framework for trusted social information management: Architecture and algorithms ," Information Sciences. vol.180, Jan.2010, pp.95-112, doi: 10.1016/j.ins.2009.06.027.

[19] M. Maheswaran, H. C. Tang, and A. Ghunaim, "Towards a Gravity-Based Trust Model for Social Networking System," Proc. of the 27th International Conference on Distributed Computing Systems Workshops, IEEE Press, Jun.2007, pp.24, doi: 10.1109/ICDCSW.2007.82.

[20] M. Taherian, M. Amini, and R. Jalili, "Trust Inference in Web-Based Social Networks using Resistive Networks," Proc. of the 3rd International Conference on Internet and Web Applications and Services, IEEE Press, Jun.2008, pp.233-238, doi: 10.1109/ICIW.2008.41.

[21] D. S. Zhai, and H. Pan, "A Social Network-Based Trust Model for E-Commerce," Proc. of 2008 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM, IEEE Press, Oct.2008, pp.1-15, doi: 10.1109/WiCom.2008.2144.

[22] I. Varlamis, M. Eirinaki, and M. Louta, "A Study on social network metrics and their application in trust networks," Proc. of 2010 International Conference on Advances in Social Network Analysis and Mining, IEEE Press, Aug.2010, pp.168-175, doi: 10.1109/ASONAM.2010.40.

[23] W. W. Yuan, D. H. Guan, and Y. K. Lee, "Improved trust-aware recommender system using small-worldness of trust networks," Knowledge-Based Systems, vol.23, April.2010, pp.232-238, doi: 10.1016/j.knosys.2009.12.004.

[24] W. W. Yuan, D. H. Guan, Y. K. Lee, and S.Y Lee. "The small-world trust network," Applied Intelligence, vol.35, Dec.2010, pp.399-410, doi: 10.1007/s10489-010-0230-7.