2011 IFIP Ninth International Conference on Embedded and Ubiquitous Computing

T-OSN : A Trust Evaluation Model in Online Social Networks

Ming Li
Deakin University
Melbourne Australia
Ming.li@deakin.edu.au

Alessio Bonti
Deakin University
Melbourne, Australia
abont@deakin.edu.au

***Abstract*—Now days, the online social networks (OSN) have gained considerable popularity. More and more people use OSN to share their interests and make friends, also the OSN helps users overcome the geographical barriers. With the development of OSN, there is an important problem users have to face that is trust evaluation. Before user makes friends with a stranger, the user need to consider the following issues: Can a stranger be trusted? How much the stranger can be trusted? How to measure the trust of a stranger? In this paper, we take two factors, Degree and Contact Interval into consideration, which produce a new trust evaluation model (T-OSN). T-OSN is aimed to solve how to evaluate the trust value of an OSN user, also which is more efficient, more reliable and easy to implement. Base on our research, this model can be used in wide range, such as online social network (OSN) trust evaluation, mobile network message forwarding, ad hoc wireless networking, routing message on Internet and peer-to-peer file sharing network. The T-OSN model has following obvious advantages compare to other trust evaluate methods. First of all, it is not base on features of traditional social network, such as, distance and shortest path. We choose the special features of OSN to build up the model, that is including numbers of friends(Degree) and contact frequency(Contact Interval). These species features makes our model more suitable to evaluate OSN users trust value. Second, the formulations of our model are quite simple but effective. That means, to calculate the result by using our formulations will not cost too much resources. Last but not least, our model is easy to implement for an OSN website, because of the features that we used in our model, such as numbers of friends and contact frequency are easy to obtain. To sum up, our model is using a few resources to obtain a valuable trust value that can help OSN users to solve an important security problem, we believe that will be big step for development of OSN.**

Keywords-component; Trust, Degree, Centrality, Contact Interval, Online Social Network, Security, Mobile Social Network, Trust community

I. INTRODUCTION

The most important factor in human social activities is trust. In fact, people making friends or making deals are based on the trust. Without the notion of trust, a high risk may be involved in our every day events. The question remains on how to evaluate trust in a digitalized world where there is a high chance that we have never met our dealing partner in real life? In realistic world, we already have some methods to evaluate trust, for example, based on the social distance. A may trust B strongly, because A has known B for a long time. And then, B introduce C to A, A may trust C base on A trust B. But A dose not trust C as much as A trust B, the reason is they have longer social distance. That is to say, a good trust is established by long-time interaction and shorter distance. The trust is also very important feature of online social network (OSN).

As we know one of the advantages of OSN is that users can make friends with other users who may comes from different a country or continent, that is beyond the traditional social network. The user could be a complete stranger. However, we have to make sure the stranger can be trusted or not, the reason is that the trust not only affects the relationship between users, but also brings security issues for them. In fact, to allow strangers or acquaintances to access a user's profile in OSN may lead to a number of privacy risks, including cyber stalking and identity theft. Features such as date of birth, gender, hometown, and address can be used for identity theft, and contact information such as email address, instant message contact name, or mobile phone can be used for stalking and spamming activities [1],Along with the OSN develop rapidly, the privacy and security problems are attracting more and more attention. Our main concern comes to solving this problem. We have researched some important features of OSN, and we believe that the trust can be used to protect people from this situation. How to use the trust and how to measure it, that is one of the purposes of this paper, which we have already tried to tackle in a previous paper [2], which is a good way to evaluate the trust value by using our model. The model calculates a trust value to represent trustworthiness of a user. A normal user only need to focus on the trust value of a strange user, if the strange user has a higher trust value that means this user is more trustworthy. Despite, there are some previous researches about trust evaluation, but most of them focus on the grid network, P2P network and reputation system. Hence these methods or

978-0-7695-4552-3/11 $26.00 © 2011 IEEE
DOI 10.1109/EUC.2011.73

models need to calculate the distance or to find the shortest path between nodes. According to our research, an individual user can make these evaluations without using these methodologies and focus more on real life social aspects, such as the interactions between node, to this extent we have focused our concerns on real OSN concepts such as a user's Degree and Contact Interval. We have built up our theoretical foundation based on the combination of these two features. The theory implies that if a user of OSN has more friends (high degree) and more frequent communication with friends (minimum contact Interval), this user can be evaluated as more secure, hence, he has a higher trust value, this value can be used by other users In our research, the main target is to build a more efficient and more reliable model to evaluate the trust value of an OSN user. To sum up, this paper will provide the following contributions:

1. Introduce the concepts of Degree Centrality and Contact Interval into OSN.
2. Build a new evaluation model of trust, to help OSN users to decrease the risk of using OSN.
3. The new model provides normal users of OSN a visualized method to evaluate the trust level of other strange users.
4. The new model and formulation can be used in widely range, such as OSN, mobile networks, ad hoc networks, traditional Internet and p2p networks.

The rest of the paper describes the new model of the T-OSN build up step by step. In section 2 introduce some work that we did. Section 3 build up the formulations and explain in details. Section 4 describes the Degree and Contact Interval concepts in OSN and the theory of T-OSN. Section 5 verifies the theory and formulations performance by using real datasets. Section 6 suggests areas for future research.

II. RELATED WORK

Trust evaluation is a more and more important issue for OSN users. In modern society, people make friends and share their interests with others by using OSN. How to measure a stranger who is trustworthy or not? To answer this question, we investigated some people who are OSN users. The most popular answer is, if people want to make friends with a stranger but they do not know this person at all, they will to find some traits which the stranger has, and these traits are close to peoples special traits. For example, they might have studied in same school or, they had worked in the same organization or, they share similar interests, perhaps they share some common friends. If the stranger has one or more traits similar to theirs, then people will think this stranger is trustworthy. In general, an OSN user needs to submit some personal information when he or she registers in OSN, other users rely on this information in order to find similar traits. However, if a stranger has a different purpose or a hidden agenda, such as acquiring information for illegitimate use, he or she may provide little or minimum information, or in some case, fake and forged information, thus it is difficult for the OSN users to measure the trust level of a stranger by using registration information only. Hence, a fraudulent user may acquire a person's trust by accepting him regardless, providing the malicious user with important information such as usernames, list of friends, in some cases even personal details such as bank accounts or important data. This can lead to further crimes, such as identity theft, even a physical attack. To find an easy way for normal OSN users to recognize other OSN users who can be trusted or not, that is our motivation to work out this research. Before we start to build our model, we did some research to evaluate the state of the current events, our survey included [3],[4],[5],[6] especially [3] as it included similar work on degree concept, in this paper, researchers built a new method (EVN) to solve the problem of message directing of distributed systems. This method was based on homophile and degree concepts. In their research, homophile represents the tendency of attributes of connected nodes to be correlated. And the degree represents that some people have a large number of acquaintances and act as hubs that connect deferent social circles. Also there are some papers focuses on trust evaluation, but most of them are focus on traditional social network, P2P network or E-commerce systems, and these models and methods to evaluate trust by using shortest path and similarities between two nodes. In other words, the past researches to evaluate the trust level between two nodes, but our purpose is deferent to theirs, ours is to evaluate trust value of one node. To conduct our new model to solve the issue of trust value evaluation, we have studied the concept of degree centrality in traditional social network [3] and the contact interval. Then we introduced these two concepts into OSN. Another source of important information was also [7], with invaluable information about users behavior in the small world theory.

There is an important question: How to combine these two concepts with OSN? There are some features of OSN, for example, the traditional degree centrality concerns the number of edges of a node, in real OSN, an OSN user instead of a node, and the number of friends represented by the edges. These similarities help us to build our new model and evaluate the formulations. In the next step, we collected user data sets of Bebo [8] to evaluate our model. In The evaluation phase, we analyzed a congruent amount of original data, the results implied that it is in fact difficult to evaluate who can be trusted more . After the calculation of 100 users data by using our mathematical model, we delivered the trust value (TL) of every use thus providing us with an effective solution. We will show the evaluation process in the "Evaluation by Using Datasets" section. In addition, we have investigated some other fields, to verify whether our model can be used or not. The conclusion is, it can be used in more fields as well. To extend our research to more technical fields will be our new target in future.

III. MATHEMATHICAL MODEL

To calculate the trust value by using our model, we assume the trust value (TL) satisfies TL ∈ [0,1]; where 1 and 0 represent complete trust success ratio and complete trust failure ratio respectively. The greater value TL is, the higher trust value the user gets. In our model, to evaluate the trust value of user x, the formula is:

Equation 1

$$TL_x = \sum \left\{ \frac{D_x}{D} * \alpha \frac{CI_x}{CI_g} * \alpha \right\} \quad (1)$$

Trust Value Calculation

$$D_g = \sum_{i>1}^{n} D_{(i,n)} \quad (2)$$

Degree of entire Graph

In the formula, D_x is the degree of user X, D_g represents the degree of the whole graph (community), CI_x denotes the contact interval of user X and the CI_g represents the contact interval of the graph (community). To carry out the contact interval, we need an additional formula, which is:

$$CI = \frac{CTs}{TCT} \beta \quad (3)$$

Contact interval calculation

The *TCT* is the total contact duration and the *CTs* is the total contact times.

.

IV. METHODOLOGY

Degree Centrality in OSN : In 1977 Freeman [9] defined the notion of degree centrality. The degree of a point is the number of other points which adjacent to this point.

In the illustration of Figure 1, the degree of point J is 1 and the degree of point A is 4. [3] The previous researches show degree is the simplest centrality measure. Applying this concept to OSN, a point is a user of OSN, the degree of an OSN user represents how many friends this user has. Assume

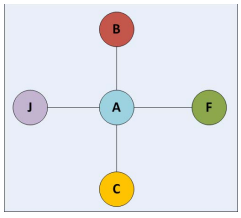

Figure 1 Degree Freeman

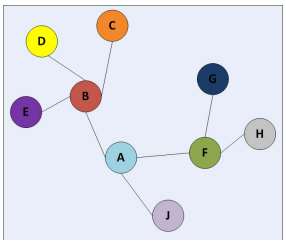

Figure 2 Degree in OSN

Figure 1 represents a small OSN, it shows user J has 1 friend A, and user A has 4 friends, they are B, C, J, F.

Contact Interval : The contact interval is the interval of communication between users of OSN. In the other words, if two users have shorter contact interval, that means they have more contact times and closer relationship. That is to say they have a higher trust relationship. In our model, firstly, we are using degree centrality to measure that whether a friend of a user of OSN can be trusted.

As the Figure 2 shows, the user B has more friends than F and J, thus A can trust B more. Secondly, as Figure 3 shows, if user A has friends B and F, B and F have same number of friends. The question is who is more trustworthy, B or F? In this case, we are considering the contact interval, if A and B have shorter contact interval than A and F, that means B is more trustworthy. However, both of those two measurements above have own drawbacks. For degree centrality measurement, as figure 2 shows, user B and F are friends of A.

User B has more friends than user F. In fact, we cannot say user B can be trusted completely. The reasons are following:

1. User B may make friends with others for some special purpose. The user B can be an attacker, with the purpose of collecting more private information, user B tries to make friends with many users. Therefore, user B has a substantial number of friends, but there are a few contacts between user B and his friends.

2. User B has some attractive features, for example, user B is using a pretty photo in his profile or published some very hot topics in OSN. These features attract people to make friends with user B. Also, there are a few contacts between user B and his friends.

For contact interval measurement, as Figure 3 shows, user B and F are friends of A, and they have the same number of friends. If A and B have shorter contact interval than A and F, but the contacts maybe focus on a particular topic during a special period. This situation represents there is an implicit trust between A and B.

In order to overcome the problems that we listed above, we combine two measurements together (Figure 4). That is to say, if user A has a friend B, B has the most friends in this community, and B has the shortest contact interval, base on these two conditions, user B has the highest trust value to user A. Hence, user B is the most trustworthy user in this community.

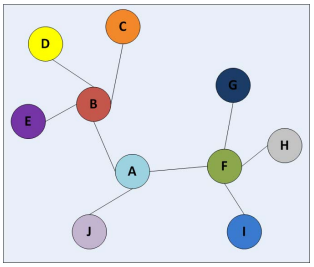

Figure 3 : Contact Interval

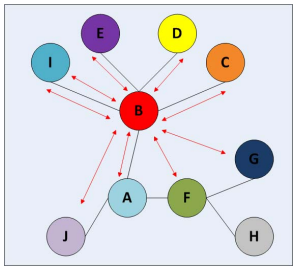

Figure 4 T-OSN

V. EVALUATION BY USING DATASETS

5.1 Data sets

The data we use in our research consists of bebo.com users in number of friends, contact frequency and registration time.

The bebo.com is a medium size online social network, which provides user a platform to make friends, write blogs and share media. This OSN is a good example for us to do our research. The figure 5 shows what the bebo.com look like.

5.2. Evaluation Results

Figure 6 shows the original data that we used, which was collected by Laszlo Gyarmati Network Economics Group in 2009 [10] In the original data, for privacy reason, username is replaced with a numerical user id. The friends value stands for the number of friends that user has. The "member since" is the user registration time and the profile views is the number of times the profile has been visited by other users. Based on this original data, it is very difficult to know which user is more trustworthy.

We then analyze the data from 100 users by using our methodology. Figure 7 shows part of our evaluation results, the results very clearly show is more trustworthy, because he or she has a higher TL(Trust value). By comparing the value of TL, we can see the user 147 has highest TL, so user 147 can be trusted more than other users.

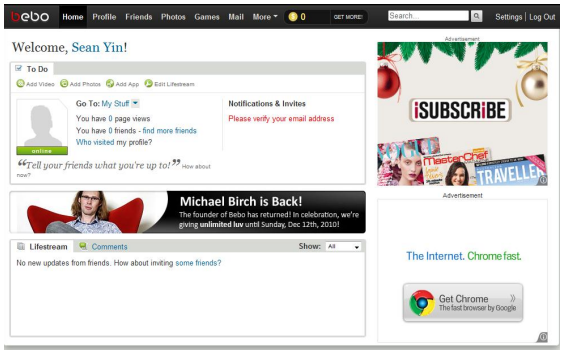

Figure 5 Bebo.com

Table 1 Original dataset

	A	B	C	D	E
1	User id	Current time	member_since	friends	profile_views
2	2	01/05/09 15:20	01/10/06	218	7713
3	3	19/04/09 20:03	01/07/06	196	2993
4	4	14/03/09 23:17	01/02/07	244	1701
5	5	15/03/09 01:57	01/03/07	439	4505
6	7	22/03/09 11:27	01/04/06	722	6424

Table 2New data produced using our model

	A	B	C	D	E	F	G	H	I
1	User id	Current time	member_since	D_x	profile_views	Total contact duration	CI_x	CI_y	TL_x
76	113	2/05/2009	1/02/2008	343	6352	456	13.93		0.158525
77	114	2/05/2009	1/08/2005	376	20170	1370	14.72		0.167561
78	115	2/05/2009	1/08/2005	420	14353	1370	10.47		0.119661
79	116	13/04/2009	1/09/2007	983	6746	591	11.41		0.131924
80	118	24/04/2009	1/07/2008	291	2473	298	8.30		0.094754
81	119	29/04/2009	1/05/2006	188	11734	1095	10.72		0.121747
82	120	15/04/2009	1/04/2007	145	12109	746	16.24		0.184063
83	121	29/04/2009	1/06/2006	261	5301	1064	4.98		0.057105
84	123	28/04/2009	1/01/2007	237	6827	848	8.05		0.091732
85	124	18/04/2009	1/04/2005	123	6127	1478	4.14		0.047226
86	125	11/04/2009	1/11/2005	366	14508	1258	11.54		0.131517
87	129	27/04/2009	1/06/2007	169	6478	697	9.30		0.105628
88	130	23/03/2009	1/07/2005	740	15612	1361	11.47		0.131834
89	131	1/05/2009	1/08/2006	373	8920	1005	8.88		0.101464
90	133	22/04/2009	1/04/2006	418	8658	1117	7.75		0.088842
91	134	2/04/2009	1/04/2006	311	5081	1098	4.63		0.053238
92	135	2/05/2009	1/03/2007	465	9537	793	12.02		0.137324
93	136	1/05/2009	1/05/2006	314	5147	1097	4.69		0.053990
94	138	30/04/2009	1/08/2005	186	5145	1369	3.76		0.043045
95	141	30/04/2009	1/01/2005	382	6875	1581	4.35		0.050283
96	143	18/04/2009	1/01/2007	219	4915	838	5.86		0.066926
97	144	13/04/2009	1/12/2005	206	21272	1230	17.30		0.196237
98	145	15/04/2009	1/08/2005	192	8316	1354	6.14		0.070029
99	147	23/03/2009	1/08/2006	344	25276	965	26.19		0.297222
100	148	20/03/2009	1/11/2006	999	7360	870	8.46		0.098518
101	153	23/03/2009	1/08/2006	202	5696	965	5.90		0.067323
102	100			34832	893106	101011		8.841627	

VI. CONCLUSIONS AND FUTURE WORK

The results show that our methodology can be quite selective in guiding an OSN user to recognize other user's trust value. This methodology can be used in some OSN to protect user's privacy and security in an easy way. It is easy to get the parameters which the formulation need and it can be implemented efficiently. As mentioned in the abstract, this methodology can be used in a wide range of fields, thus our future work will pay greater attention to the extent to other topologies, for example, to calculate the hotter router by using our model to improve routing protocol and to help message forwarding system to choose next hop, which will be a new choice for the existing network systems.

REFERENCES

[1] 1. Kolaczek, G. An Approach to Identity Theft Detection Using Social Network Analysis. in Intelligent Information and Database Systems, 2009. ACIIDS 2009. First Asian Conference on. 2009.

[2] 2. Ming, L. OST: A Transaction Based Online Social Trust Model for Social Network and File Sharing Security. 2010.

[3] 3. Şimşek, Ö. and D. Jensen. Navigating networks by using homophily and degree. 2008: Proceedings of the National Academy of Sciences.

[4] 4. Bogu, et al., Models of social networks based on social distance attachment. Physical Review E, 2004. **70**(5): p. 056122.

[5] 5. Jin, S. and A. Bestavros. Small-world characteristics of the Internet and multicast scaling. in Modeling, Analysis and Simulation of Computer Telecommunications Systems, 2003. MASCOTS 2003. 11th IEEE/ACM International Symposium on. 2003.

[6] 6. Hao, L., H. Kuo-Chan, and H. Hung-Chang. *Small-World Social Relationship Awareness in Unstructured Peer-to-Peer Networks*. in *Parallel and Distributed Systems (ICPADS), 2010 IEEE 16th International Conference on*. 2010.

[7] 7. Watts, D.J., *Small Worlds:The Dynamics of Networks between Order and Randomness*. 2003.

[8] 8. Bebo. *Bebo*. 2011; Available from: www.bebo.com.

[9] 9. Freeman, L.C., *A Set of Measures of Centrality Based on Betweenness.* Sociometry, 1977.

[10] 10. Gyarmati, L. and T. Tuan Anh, *Measuring user behavior in online social networks.* Network, IEEE, 2010. **24**(5): p. 26-31.

[11]