Trust Evaluation in Unsupervised Network: A Fuzzy Logic Approach

Golnar Assadat Afzali
Department of Industrial Engineering, K. N. Toosi University of Technology, Tehran, Iran
gafzali@kntu.ac.ir
Monireh Hosseini*
Department of Industrial Engineering, K. N. Toosi University of Technology, Tehran, Iran
hosseini@kntu.ac.ir

Received: 15/Apr/2013 Revised: 20/May/2014 Accepted: 21/Jul/2014

Abstract
Because of the possibility of anonymity and impersonation in social networks, trust plays an important role in these networks. In social networks, trust can have two aspects: trust of users to social network and trust of users to other users. Pear to pear networks, by eliminating the supervisor roles, besides its benefit in decreasing management costs, have problems in trust and security of users. In these networks, trust evaluation is only related to the trust of pear to other pear and because of the direct relation between pears; each user should know the trust level of other users. However, trust evaluation in pear-to-pear networks (as an unsupervised network), only can be done based on the past relation between pears or trust evaluation of other pears. This kind of trust evaluation cannot give a comprehensive view to pears. In other word, if any pear is not in the friend cycle of a user or friend cycle of user's friends, he will not be able to assign appropriate trust level to this pear. In this research, by using social networks as supervised networks, trust level of each user is evaluated, then by identifying these users in unsupervised networks, appropriate trust level is assigned to them.

Keywords: Trust; Unsupervised Networks; Trust Factors; Fuzzy Logic.

1. Introduction

With increasing growth of using internet, users confront with many problems in security and privacy [1,2,3,4]. Due to the lack of face to face relationships and simplicity of impersonation in these networks, distribution of incorrect information is increased [5,6]. So, considering only shared information of users cannot be a good criterion for measuring trust. Therefore, trust and evaluation of user's trust level is taken into consideration [5,7,8,9,10]. In general, trust is influenced by many factors, such as shared information of user, past interactions with his, positive or negative comments of other users and etc. [11]. Besides, trust in unsupervised networks, -such as pear-to-pear networks- is more sensitive. In these networks, lack of supervision makes tracking user's behavior impossible. On the other hand, because of the nature of activities in these networks, trust is more important. For example, in many cases, users allow others to run programs on their systems; therefore, inappropriate behavior of users can cause serious problems. Many researches have been done on trust in unsupervised networks [12,13,14,15]; nevertheless, in most of them, trust is considered as a static parameter. This means that calculation of user A's trust in time t, would be done based on accessible data about him on that time, such as shared information in his profile, affiliations and membership information of groups. But in real, trust is a dynamic concept and in addition to considering its static aspects, it must be updated during time and based on user's activities.

In this paper, with considering both static and dynamic aspects of trust, the trust level of users would be determined. Then by identifying user on other unsupervised networks, his trust level would be assigned. Therefore, reliable and secure relationships can be established in these networks.

The reminder of this paper is organized as follow: Section 2 provides definition of trust and an overview on related researches in trust. In section 3, after specifying trust factors, related weights are computed. Then, in section 4, evaluated trust in supervised networks is used to predict appropriate trust level of user in unsupervised network. At last, section 5 concludes the paper.

2. Related work

2.1 Trust

Trust is a critical component in human relationships and consequently in social networks [16]. In general definition, trust is a measure of confidence that an entity will behave in an expected manner [17]. Trust-based community is a community that people can share their opinions without any concern about privacy or false judgment of others. Social trust is concerned as a foundation for creating trust-based community in social networks [18]. Social trust is influenced by many factors,

* Corresponding Author

such as past experiences with user, opinion of other users about him, psychological factors and etc. [17]. Difficulty of defining trust and converting it into quantifiable format causes problems in combining trust with algorithms and mathematical analysis [18]. Trust is an asymmetric parameter, means that in a relationship, the trust level of two nodes can be different. Also, trust is a context-aware concept and dynamic [19].

Many researches have been done on trust. PearTrust model [19], tries to determine trust level of users based on three parameters and two adaptive factors. The parameters are received feedbacks from other users about him, transactions and assigned trust level to him by others. The factors are the context of transactions and network environment.

Walter et al. [20], tried to calculate indirect trust between users based on the direct trust between neighbor nodes in social networks. For this, any node can assign a trust level to other nodes in [-1, 1]. Finally, based on the recommended trust level of any neighbor node and the weight of link between them, user's trust level is determined.

The proposed model of Borbora et al. [10], shows that factors such as shared personal information, node's location within network and other social interactions with nodes in this social network are the most trust influencing factors between users.

New algorithm proposed in Xin et al. model [21], uses indirect trust between users. Indirect trust value is determined depending on direct trust values and trust chain between users that are not neighbors. In this algorithm any node can rate other's trust value in [0, 1].

2.2 Trust in unsupervised social network

Trust in supervised and unsupervised networks has fundamental differences. In unsupervised networks, trust is determined in absolute correct parameters. A file either is impaired or not. A protocol is entirely implemented or not. However, in supervised networks, trust value can have a wide range [22].

In the proposed model of Wang et al. [23], a trust matrix is considered, which any node can rate other nodes. So, any node can easily evaluate each node based on others rates.

Huang et al.[24], emphasize on the role of feedback in building trust between users. In these systems, usually assumed that normal pears can have standard and ideal feedback behaviors. In this paper, instead of direct feedback from users, duration that downloaded file remains in the shared folder is used to determine trust level.

Zhen-wei et al. [25], based on general characteristics of trust between P2P networks (as unsupervised networks) and social networks (as supervised networks), proposed a model to evaluate trust in social networks and utilized it in P2P networks. So, based on user past performance, trust degree is calculated and then assigned to user in P2P network. In this model, static 0-1 view is obvious. However, by using fuzzy logic approach, trust evaluation would be more précised [26]. For example, it is possible that two users which are in the same trust level have high difference; but with membership degrees, these differences would be more perceptible. In fuzzy logic approach, trust evaluation would be based on a vector of membership degrees related to each trust level.

In [27], Han et al. proposed a topological potential weighted community-based recommendation trust model (IPCommuTrust). In this model, besides considering node's reputation, its status would be effective in determining its trust level. Status of node is based on the shortest path between them.

Yu et al. [28], proposed a model to provide trust evaluation in social network. In this model, trust level of user would be determined based on the referral trust evaluation is given to any requestor user and this can be used beside user's prior experiences. Both direct and indirect trust evaluation will be updated during time.

Li et al. [29], with defining trust as a complex and multi-dimensional parameter, tried to determine these dimensions and effective weights related to them. The main advantage of this model is that trust degree assigned to each user could be changed over time by updating the weights. It should be considered that the mentioned problem in [25], also exits in this proposed model.

The proposed model in [13], contains three factors including quality, popularity, and size of the shared file as trust factors. Then, a fuzzy inference system is used to design P2P reputation management system, which generates the reputation values for users by interacting with other peers, and based on these factors.

In [14], Chen et al., proposed a two-part model containing direct trust and the assigned trust by other users. Once mutual peers recognize each other, they can evaluate other's trust level. In cases which peers don't recognize each other, they could use other's recommendations. This model easily could be hacked. Consider the case that hacker "A" wants to hack user "B". At first step, A gets in the relationship with some friends of B and tries to increase his trust level in their relationship with his trustworthy behaviors. Now, in direct relationship between A and B, because of not existing of mutual recognition, trust evaluation would be done based on mutual friends. So, user A can easily hacks user B.

In our model, trust would be evaluated based on defined trust factors, which each has an appropriate weight, and with appropriate weights for each of them. Due to unawareness of hackers of these factors and their related weights, they could not increase their trust level by fake information. The problem, which exits in many related research studies, is the static consideration of trust. However, trust is a dynamic parameter and should be updated over time. In this paper, trust is considered as a dynamic parameter. So, fake behaviors of users in period of time for getting high level of trust don't have an essential effect on evaluated trust. Table 1 summarizes related works in this manner.

3. Proposed model for computing trust in unsupervised networks

As mentioned, social networks with their virtual relationships increase the importance of trust factors determination. On the other hand, because of not existence of supervisor in unsupervised networks, an integrated view of user's behavior would not be available. To solve this problem, the role of supervisors in supervised networks can be used to evaluate trust level of users and then the results will be used in unsupervised networks. Our proposed model is based on the pattern demonstrated in figure1.

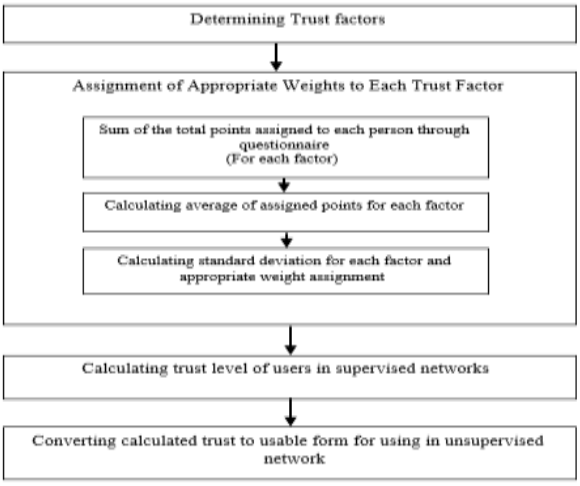

Fig 1. Considered steps of the proposed model

Table 1. Summary of related works

Reference	Publish year	Main purpose	Addressed issues	Not addressed issues
[20]	2009	Determining effective factors in trust	-Node location in network (relation) - Node properties such as personal information, activity related to other users (for example sending message to others)	-Inter-activity (such as updating his profile, etc.) -Behavioral (long-term performance of user interacting with other users)
[13]	2009	Trust evaluation between non-adjacent nodes	-Personal information -Behavioral	-Intra-activity (activity related to other user, such as sending message to others) -Inter-activity
[25]	2010	Trust evaluation between non-adjacent nodes by trust chain between users and the trust of user to his friends	-Reputation (personal information) -Behavioral	-Inter-activity -Intra-activity
[12]	2011	Effective factors in trust	-Personal information -Inter-activity -Intra-activity -Relation	-Behavioral
[29]	2011	Users' feedback for evaluating trust	-Feedback of users, based on retention time of downloaded files in shared folder	- Personal information -Inter-activity -Intra-activity -Behavioral -Relation
[7]	2012	Determining trust level of users in social networks and using it in P2P networks	-Personal information -Behavioral	-Relation -Inter-activity -Intra-activity
[24]	2012	Trust evaluation and updating it by considering dynamic weights for its effective factor	-Feedbacks of other users -Intra-activity -Behavioral -Risk of interaction -Availability of user	-Inter-activity -Relation
[21]	2013	Using fuzzy logic to form trust vector for any shared file by user	- Attributes of shared files (quality, popularity, size of file)	-Personal information -Inter-activity -Intra-activity -Relation -Behavioral
[10]	2013	Trust evaluation using two approach: direct trust (based on past interaction of users), indirect trust (a mutual and trusty node)	-Behavioral	-Personal information -Inter-activity -Intra-activity -Relation
[27]	2014	Trust evaluation using reputation and status of users.	-Relation -behavioral	-Personal information -Inter-activity -Intra-activity
[28]	2014	Trust evaluation based on direct past experience and recommendation from corresponding recommendation peers	-Behavioral	-Personal information -Inter-activity -Intra-activity -Relation
Proposed model		Trust evaluation in supervised network and using it in unsupervised networks	-Personal information -Inter-activity -Intra-activity -Relation -Behavioral	- Feedbacks of other users

3.1 Trust factors determination

Fong et al. [7], in order to determine trust factors, have proposed a hierarchy similar to "trust model" which considered in the model of Gilbert et al.[30]. This hierarchy is included all trust factors in an acceptable level. The main problem in this model is the static view of trust, regardless of the user's past behavior. For this, we will extend this hierarchy with considering behavioral factor. So, our model will be based on the hierarchy similar to figure 3. Each of the factors will be described in detail in the next section.

3.1.1 Analytical factors

3.1.1.1 Relation

In this factor, the relation link between two nodes i and j is regarded as the criterion for rating friends. So, the trust network is plotted. In this network, each relation between nodes will be drawn with a weighted link. This weight can be assigned based on the type of relation between them [7]. For example, in figure 2, node i determines node j as a "close friend". So, the weight of this link can be equal to 5. In this network, two points should be considered:

- Number of weights, which assigned to each group of friends, does not have any effect on solution comprehensiveness. The only notable matter is that all of these weights should be assigned based on the same pattern (similar to table 2).
- Trust evaluation in this network will be done base on the shortest path between two nodes i and j.

Table 2- An example of relation link weighting in trust network

Type of relation	Weight
Family	6
Close friend	5
Friend	4
Co-worker	3
Friend of friend	2
Others	1

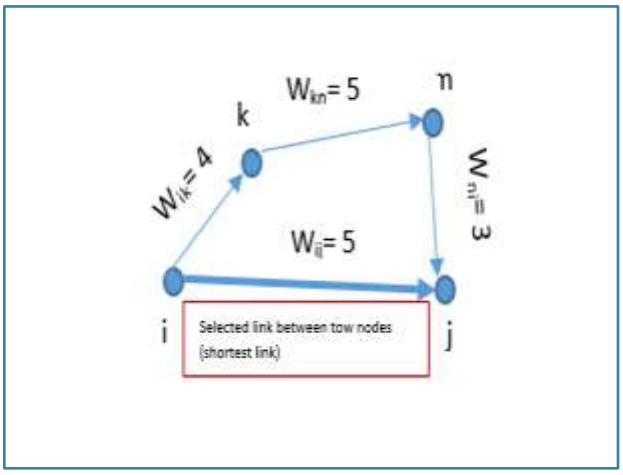

Fig 2. Calcualting relation factor in trust evaluation

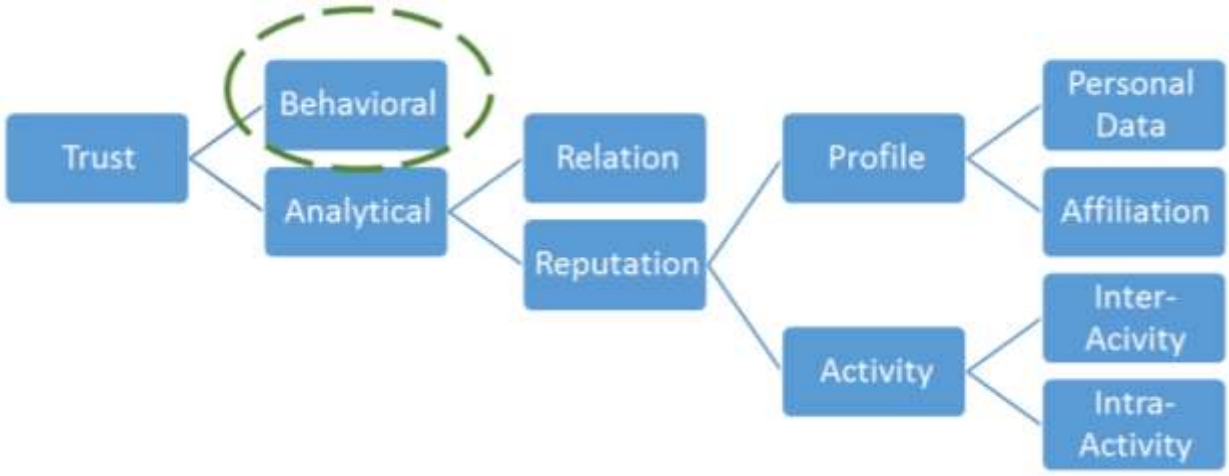

Fig 3. The proposed trust hierarcy

3.1.1.2 Reputation

This factor usually emphasizes on the opinion of others about any user. In social networks, because of the virtual form of relations, this parameter can have an important role. This attribute is related to personal information in user's profile and history of s activity. So, this factor can be studied in two parts: "profile" and "activity"[7].

- Profile:
  This factor mainly focuses on the effect of user's profile on others mindset. This information can present user's affiliation besides personal attributes [7, 22, 25].
- Activity
  User activities are divided in two categories: inter-activity and intra-activity. Inter-activities are related to user's activities such as personal posts,

comments provided on topics and etc. However, intra-activities are activities such as post on other's wall, visiting other's profile and etc. [7, 10].

3.1.2 Behavioral

Behavioral factors considered to add dynamic aspect to analytical factors. The main idea of these factors is related to the dynamic treat of trust. In other word, considering only personal information or user's affiliations cannot be acceptable for trust evaluation; but user activity should be tracked over time [13,20,21,25,29]. This factor consideration, in addition to ensure reasonable trust evaluation, will increase system security. A known attack is that, hacker increases his trust level by providing appropriate values for each trust feature. But, with behavioral factors, besides these features, real behavior of any friend is tracked. So, this kind of attacks can be prevented by using this factor.

3.2 Factors weighting

In previous section, trust factors were determined. Now, the appropriate weights of each factor should be calculated. So, with a questionnaire, some users of social networks were asked to with considering five trust levels, such as "high trusty, trusty, no comment, almost untrusted, untrusted ", assign at least one of their friends to each level and answer to the related questions.

After gathering questionnaire results, weight of each factor is determined. Then, based on formulas 1, 2, and 3, trust degree of users are calculated and finally the range of each trust level is shown by a fuzzy membership function.

Suggested questionnaire has five subdivisions and each of them is related to one of the trust factors. If users which participate in our questionnaire are shown with P_j (j=1,2,..,r) and friends which assigned by users in each trust level are shown with P_{jm}(m=1,2,3,4,5), for each trust factor, appropriate values are assigned to each P_{jm}, based on the answers of P_j in each related subdivision. At first, in order to extract rules about trust factors in any trust level, users with different trust level are considered as an integrated set, regardless of their trust level. To evaluate factor's weight, for all P_{jm}, sum of each factor value are calculated and then the related average is calculated based on formula 1.

$$\lambda i = (\sum_{j=1}^{r} \sum_{m=1}^{5} (Pijm))/n \quad (1)$$

In formula 1, λ_i is the average of factor i, P_{ijm} is the value of factor i for user P_{jm} and n is the number of all P_{jm}.

At last step, by calculated average in formula1, the standard deviation is computed using formula 2.

$$\delta I = \sqrt{\frac{1}{n} * \sum_{j=1}^{r} \sum_{m=1}^{5} (Pijm - \lambda i)^2} \quad (2)$$

In formula 2, δ_i is the standard deviation of factor i, P_{ijm} and λ_i, similar to formula 1, are user's value and average related to factor i.

Now, based on calculated standard deviation, appropriate weight is assigned to each factor i. In other word, standard deviation can express the importance of each trust factor. More precisely, standard deviation of each factor demonstrates the cohesion of users on this factor. So, if this value is low, it could be concluded that most of users are approximately same in this factor and this weight should be more and if the standard deviation is high, related weight should be low. Table 3, can be used as a criterion for factor weighing.

Table 3. Weight assignment based on standard deviation

δ	W
0 – 0.2	1
0.2-0.4	0.9
0.4-0.6	0.8
0.6-0.8	0.7
0.8-1	0.6

Finally, by formula 3, trust degree of each user is calculated.

$$T_{jm} = \sum_{i=1}^{k} Wi(|\frac{Pijm - \lambda i}{\lambda i}|) \quad (3)$$

In formula 3, T_{jm} is the trust degree of user P_{jm} and P_{ijm}, λ_i and W_i are user P_{jm} trust value, average of factor i and the weight of factor i, respectively. K is the number of trust factors. (In proposed model, k is equal to 6.)

3.3 Implementation of the proposed method

To collect required information, a questionnaire is considered which can cover all of the trust factors. The questionnaire was distributed among users of Facebook (as a supervised network) and users were asked to with considering the five trust levels (defined in section 3-1), assign one of their fiends to each level and answer to the questions. Finally, based on these results, appropriate trust degree assigned to each friend.

3.3.1 Sample size

In order to ensure the accuracy of sampling and generalizability of results to the other users, sample size should be large enough. There are several methods to determine the sample size. The two most popular methods are Morgan table and Cochran formula. In this research Cochran formula is used. Based on this formula [31], if the population size cannot be determined exactly, the sample size is calculated according to formula 4.

$$n = \frac{pqz^2}{d^2} \quad (4)$$

In formula 4, n determines sampling size, P is the estimation proportion of an attribute that is present in the population, d is the acceptable sampling error, z is the abscissa of the normal curve of that cuts off an area α at the tails and q is the proportion of the attribute that absence in the population.

In this research, due to not clearing the number of joint members of supervised and unsupervised networks whom are suitable for applying the model on them, each

of p and q values are considered equal to 0.5, d value is considered equal to 0.0.1 and z value is considered equal to 1.96. By these assumptions, based on formula 4, the appropriate sample size would be equal to 96.

3.3.2 Recommended weights for each factor

As explained, the questionnaire was distributed among 96 users. Based on results and formulas, which mentioned in section 2-3 and table 3, results such as average, standard deviation of each factor and finally, the range of trust degree for each trust level, are shown in tables 4, 5 and 6.

Table 4. Calculated avarage of each factor

Feature	Average
Relation	0.366
Personal information	0.633
Affiliation	5.333
Inter-activity	10.055
Intra-activity	10.333
Behavioral	3.111

Table 5. Standard deviation and weight of each factor

Feature	Standard deviation	Weight
Relation	0.277	0.9
Personal information	0.147	1
Affiliation	0.620	0.7
Inter-activity	0.429	0.8
Intra-activity	0.403	0.8
Behavioral	0.233	0.9

Table 6. Range of each trust level

Trust level	Min	Max
Untrusted	317	325
Almost untrusted	323	334
No comment	332	362
Trusty	353	391
High trusty	389	401

3.4 Trust assignment in unsupervised networks

As mentioned, in unsupervised networks, because of the ease of impersonation, not existence of supervisors and the direct and great impact of user behavior on others, trust has an important role in these networks. So, we're going to assign a trust level to users of these networks, based on the evaluated trust in past section. The problem that arises in this matter is that the evaluated trust is in the format of a number and in other networks, this number cannot easily express the trust level of users. To solve this problem, fuzzy logic and especially, membership function can be useful. For this, based on the questionnaire results and formulas in section 3-2, final trust degree of each user is calculated and based on the assigned trust level, range of each trust level is defined and can be shown by a membership function. Figure 4 shows the suggested membership function.

In figure 4, vertical axis represents the membership degree of fuzzy variable and horizontal axis represents the calculated trust degree based on formula 3. In this figure, the membership functions are related to "untrusted", "almost untrusted", "no comment", "trusty", and "highly trusted", respectively. By these functions, the membership degree of trust variable to each trust level is determined as a vector in the form of [untrusted, almost untrusted, no comment, trusty, highly trusted] and trust evaluation would be based on this vector. For example in figure 4, trust vector of user "A" would be as follow:

E_a= [0.4, 0.4, 0, 0, 0]

4. Implication

As an example of proposed solution, trust evaluation and authentication of users can be considered. To do so, the following steps can be considered:

1. User P_1 as a member of network N_1, sends a request to communicate with another user of this network, P_2.
2. User P_2 needs to evaluate trust degree of P_1. So, related information about membership of P_1 in supervised networks, are asked to be sent to P2.
3. User P_1 sends his membership information to P_2.(IP_1)
4. User P_2 sends IP_1 to "Trust Center (TC)" and requests to evaluate his trust level.
5. Sending membership information of P_1 to all related networks.
6. Specification of considered factors in trust evaluation and determining trust level of user P_1 and forwarding these evaluations to the trust center (TC).
7. Aggregating factors and computing total trust based on the formula 3 and then creating trust vector.
8. Sending result to the P_2 by TC.
9. Accept or reject the request of user P_1.

In figure 5, all of the above steps are shown.

Example of implication:

1. Alice wants to communicate with Bob on Skype (as an unsupervised network). So, she sends her request to Bob.
2. Before any communication, Bob needs to verify Alice and evaluate her trust level. So, he asks her to send her membership information in supervised networks such as Facebook, Twitter and etc.
3. She sends her membership information (such as her ID) of supervised networks, such as Facebook and Youtube.
4. Bob sends Alice's membership information to "Trust Center" and requests to evaluate her trust level.
5. Trust Center sends her membership information to the related networks and asks them to evaluate her trust level.
6. Each of these networks (Facebook and Youtube) sends its calculated trust degree. Beside this, they should send factors which considered for trust evaluation.
7. "Trust Center" aggregates these factors and evaluates final trust based on the received results.
8. Final trust vector will be sent to Bob.
9. Bob decides to accept or reject Alice.

5. Conclusions

Nowadays, social networks have created new challenges in security and trust. Besides, unsupervised networks, because of the not existence of supervisors and high level of access in some cases, such as access to run a program on other user's system, trust has a more important role. Many researches have been done on this problem, but static view of trust in most of them, causes failure in hacker identification. In more detail, because of the lack of supervisors in these networks, observing the behavior of nodes in relation with other nodes cannot be possible. While, in supervised networks, the supervisor can record all of the user behavior and assign appropriate trust level, based on them. In this research, with the purpose of providing a dynamic model for trust evaluation in unsupervised networks, supervisor roles in supervised networks are used. Based on the behavior of users in these networks and their shared information, appropriate trust degree is assigned to them. After drawing membership function of each trust level, the trust vector of user is determined based on the membership degrees and can be used to evaluate the trust level of him.

The limitation of this research is related to the manual submission of membership information in the supervisor networks for user authentication. In future, works, with the automatic version of this part, analyzing the whole behavior of users in all networks which they are membered in, can be possible and user cannot hide his bad behavior in some networks.

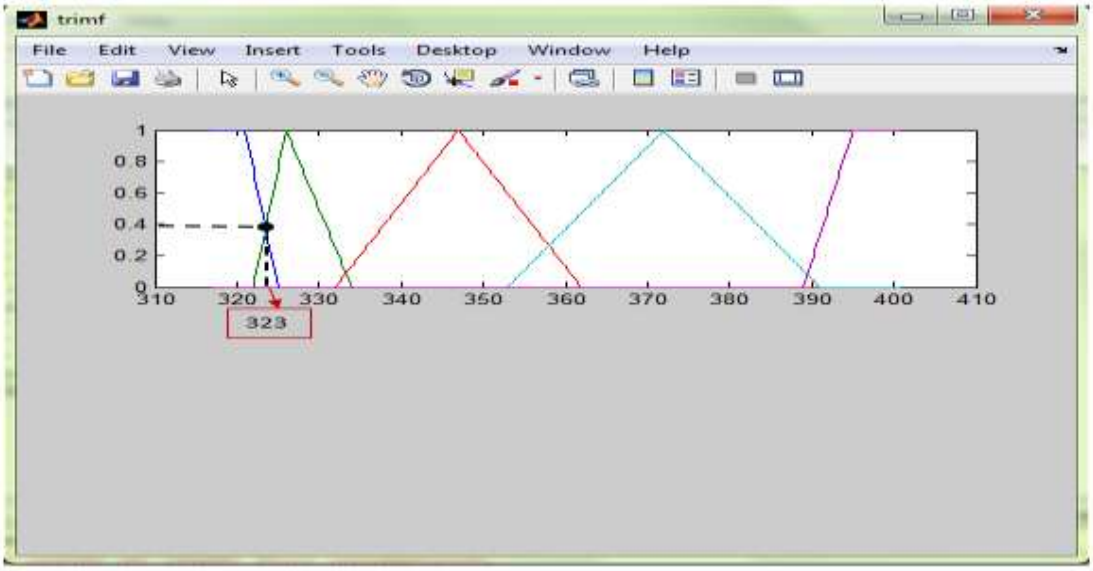

Fig 4. The membership function of trust level variable.

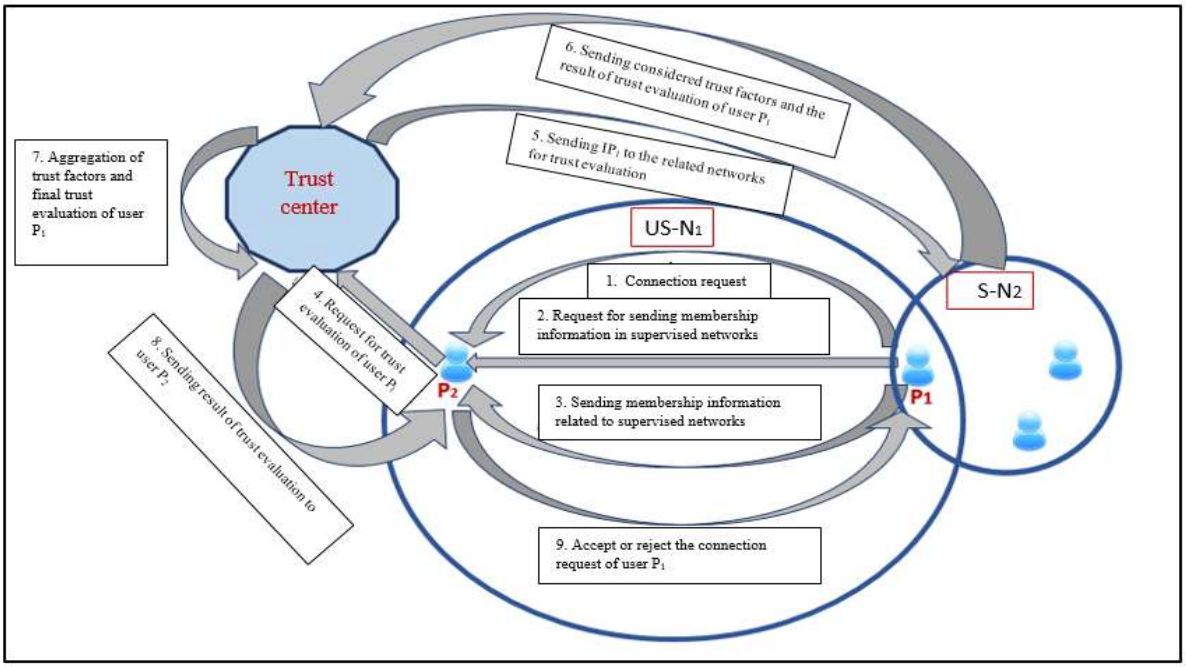

Fig 5. The framework for application of the proposed model

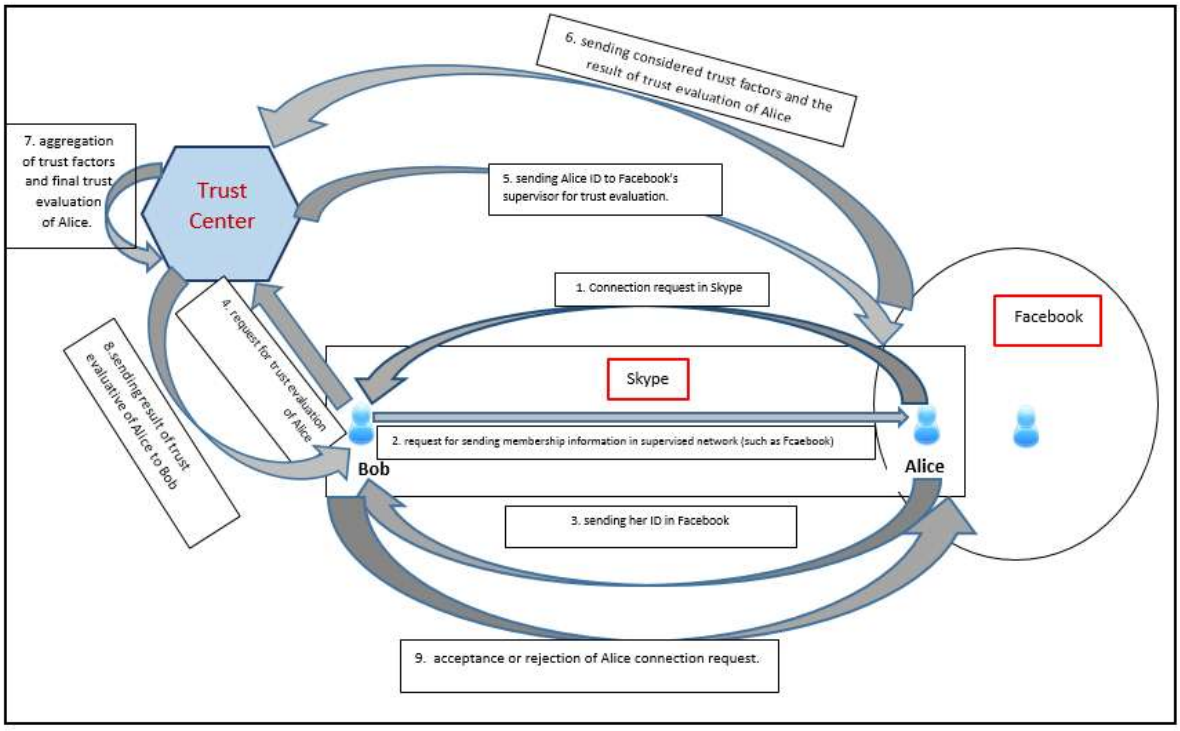

Fig 6. A real-world example of the proposed model

References

[1] Adali, S., Escriva, R., Goldberg, M.K. , Hayvanovych, M., Magdon-Ismail, M., Szymanski, B.K., Wallace, W.A., Williams, G., "Measuring Behavioral Trust in Social Networks", Third American Conference on Information System, IEEE, pp 150-152, May 2010.

[2] Wondracek, G., Holz, T., Kirda, E., Kruegel, C., "A Practical Attack to De-Anonymize Social Network Users", IEEE Symposium on Security and Privacy (SP), pp 223-238, May 2010.

[3] Zhang, C., Sun, J., Zhu, X., Fang, Y., "Privacy and Security for Online Social Networks: Challenges and Opportunities", IEEE Network, Vol.24, No.4, pp13-18, 2010.

[4] Pisey, S.H., Ramteke, P.L., Deshmukh, P., Burghate, B.R., "Privacy Access Control Mechanism for Online Social Network", International Journal of Computer Science and Applications, Vol.6, No.2, pp 172-179, April 2013.

[5] Nagy, J., Pecho, P., "Social Networks Security", Third International Conference on Emerging Security Information, System and Technologies, pp321-325, June 2009.

[6] Livingstone, S., Brake, D., "On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications", Children and Society, pp 75-83, Vol. 24, No.1, Jan 2010.

[7] Fong, S., Zhuang,Y., Yu, M., Ma, I., "Quantitative Analysis of Trust Factors on Social Network using Data Mining Approach", International Conference on Future Generation Communication Technology(FGCT), IEEE, pp 70-75, Dec 2012.

[8] Liu, G., Wang, Y., Orgun, M.A., "Social Context-Aware Trust Network Discovery in Complex Contextual Social Networks", Association for the Advancement of Artificial Intelligence, 2012.

[9] Huang, B., Kimmig, A., Getoor, L., Golbeck, J., "A Flexible Framework for Probabilistic Models of Social Trust", 6th International Conference on Social Computing, Behavioral-Cultural Model and Prediction, pp 265-273, 2013.

[10] Borbora, Z.H., Ahmad, M.A., Oh, J., Haigh, K.Z., Srivastava, J., Wen, Z., "Robust Feature of Trust in Social Network", Social Network Analysis and Mining. Vol.3, No.4, pp 981-999, 2013.

[11] Dwyer, C., Hiltz, S.R., Passerini, K., "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace", International Conference on Intelligence and security informatics, August 2007.

[12] Mahapatra, A., Tarasia, N., "A Fuzzy Approach for Reputation Management using Voting Scheme in Bittorrent P2P Network", International Journal of computer science and information technologies, Vol .2 , No.2, pp735-740, 2011.

[13] Chen, H., Ye, Zh., Liu, W., Wang, Ch., "Fuzzy Inference Trust in P2P Network Environment", International Workshop on Intelligent System and Applications, pp 1-4, 2009.

[14] Biao, C., Zhishu, L., "Computing and Routing for Trust in Structured P2P Network", Journal of Networks, Vol.4, No.7, pp667-674, September 2009.

[15] Sandhya, S., "Trust Management in P2P Networks using Mamdani Fuzzy Inference Systems", International Journal of Computer Application (IJCA), Vol. 66, No.14, March 2013.

[16] Sherchan., W., Nepal, S., Paris, C., "A Survey of Trust in Social Networks", ACM Computing Surveys (CSUR), Vol.45, No.4, August 2013.

[17] Golbeck, J., Hendler, J., "Inferring Binary Trust Relationships in Web-Based Social Networks", ACM Transaction on Internet Technology (TOIT), Vol. 6, No. 4, November 2006.

[18] Bharadwaj, K.K., Al-Shamri, M.Y.H., "Fuzzy Computational Models for Trust and Reputation Systems", Electronic Commerce Research and Application, Vol.8, No.1, pp 37-47, 2009.

[19] Xiong, L., Liu, L., "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities", IEEE Transaction on Knowledge and Data Engineering, Vol.16, No.7, pp843-857, July 2004.

[20] Walter, F.E., Battiston, S., Schweitzer, F., "Personalised and Dynamic Trust in Social Networks", Third ACM Conference on Recommender Systems, pp 197-204, 2009.

[21] Xin, L., Leyi, S., Yao, W., Zhaojun, X., Wenjing, F., "A Dynamic Trust Conference Algorithm for Social Network", Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), pp 340-346, Oct 2013.

[22] Taherian, M., Amini, M., Jalili, R., "Trust Inference in Web-Based Social Networks using Resistive Networks", Third International Conference on Internet and Web Applications and Services (ICIW), pp233-238, June 2008.

[23] Wang, H.Y., Zhao, Y.F., Meng, X.D., Ji, X.J., "Achieving Quick Trust Transmission in P2P Network Based on Matrix Operation", Manufacturing Engineering and Process II, June 2013.

[24] Huang, Z., Lu, S., Zhang, A., Gu, J., "Impact of Feedback on Trust in P2P Network", Journal of Networks, Vol. 7, No.8, pp 1182-1188, Aug 2012.

[25] Zhen-wei, Y., Qing-guo, S., Jun, L., "A Trust Evaluation Approach for P2P Nodes Based on Trust Computing ", 12th IEEE International Conference on Communication Technology (ICT), pp 1088-1091, Nov 2010.

[26] Zadeh, L.A., "Toward a Theory of Fuzzy Information Granulation and its Centrality in Human Reasoning and Fuzzy Logic", Fuzzy Sets and Systems journal, Vol.90, pp 111-127, 1997.

[27] Han, Q., Wen, H., Ren, M., Wu, B., Li, S., "A Topological Potential Weighted Community-Based Recommendation Trust Model for P2P Networks", Peer-to-Peer Networking and Applications, June 2014.

[28] Yu.Z., Zhu.J., Shen.G., Liu,H., "Trust Management in Peer- to-Peer Networks", Journal of Software, Vol.9, No.5, pp 1062-1070, May 2014.

[29] Li, X., Zhou, F., Yang, X., "A Multi-Dimensional Trust Evaluation for Large-Scale P2P Computing", Journal of Parallel and Distributed Computing, Vol. 71, No. 6, pp837-847, June 2011.

[30] Gilbert, E., Karahalios, K., "Predicting Tie Strength with Social Media", SIGCHI Conference on Human Factors in Computing System, pp 211-220, 2009.

[31] Cochran, W.G., "Sampling Theory When the Sampling Units Are of Unequal Sizes", Journal of American Statistical Association, Vol.37, No.218, Jun 1942.

Monireh Hosseini holds a PhD from Tarbiat Modares University (TMU). She is currently an assistant professor at the Information Technology Department of Industrial Engineering Faculty at K. N. Toosi University of Technology. Her work deals with customer analytics and network models of customer value. She has teaching experience in Internet marketing, ecommerce strategies and Management Information Systems. She has published a number of research papers in international scientific journals and conference proceedings. She is the highly commended winner of the 2011 Emerald/EFMD Outstanding Doctoral Research Awards and received two scientific awards for the best paper in March 2008 and January 2011.

Golnar Assadat Afzali is a master student of Information Technology Engineering at K. N. Toosi University of Technology. She received her B.S. degree in information technology engineering from Isfahan University of Technology (IUT). Her work deals with network models of trust and information security.