Kybernetes

Trust evaluation between the users of social networks using the quality of service requirements and call log histories

Parina Alamir Nima Jafari Navimipour

Trust evaluation between the users of social networks using the quality of service requirements and call log histories

1. Introduction

Nowadays with the rapid progress of distribution systems such as grid computing (Navimipour & Khanli, 2008; Souri & Navimipour, 2014), cloud computing (Chiregi & Jafari Navimipour, 2016; Navimipour, 2015b; Navimipour & Milani, 2015), peer-to-peer networks (Navimipour & Milani, 2014), expert cloud (Ashouraie & Jafari Navimipour, 2015; Hazratzadeh & Jafari Navimipour, 2017; Jafari Navimipour, Masoud Rahmani, Habibizad Navin, & Hosseinzadeh, 2014; Jafari Navimipour, Rahmani, Habibizad Navin, & Hosseinzadeh, 2015; Navimipour, 2015a; Navimipour, Rahmani, Navin, & Hosseinzadeh, 2015; Navin, Navimipour, Rahmani, & Hosseinzadeh, 2014), electronic management (Navimipour & Soltani, 2016; Navimipour & Zareie, 2015; Soltani & Navimipour, 2016; Zareie & Jafari Navimipour, 2016; Zareie & Navimipour, 2016), and knowledge management (Charband & Navimipour, 2016; Jafari Navimipour & Charband, 2016) social networks are increasingly attracting the attention of people from all around the world via powerful communications (Sharif, Mahmazi, Navimipour, & Aghdam, 2013). Social networking service is a popular service which provides a platform for people to create profiles and shares contents with other people (Fan & Yeung, 2015). Every day Millions of people are joining social networks, interacting with others they did not know before (Jiang, Wang, & Wu, 2014). Therefore, people in social networks, restrict their information; and the sharing of this information is becoming more closed, making social network services lose their original benefits (Al-Oufi, Kim, & El Saddik, 2012). In a virtual environment where participants are usually anonymous and do not engage in direct face-to-face communication, trust can be a very significant issue (Zolfaghar & Aghaie, 2011). Participants in social networks want to share information and experiences with as many reliable users as they have in their network while inhibiting malicious users from accessing their personal information (Al-Oufi et al., 2012). However, the enormous growth of social network sites in recent years has led to unreliable users who misuse these services by committing acts considered as privacy violation (Dwyer, Hiltz, & Passerini, 2007). Social networking has become a popular activity in today's Internet world, with billions of people across the world using this media to meet old friends, make new friends, and collect and share information. The social network is a popular media but has several disadvantages associated with it. Scammers or hackers leading to a lose of confidentiality and identity theft of the users can trap these sites. In addition, there are many challenges like fake profiles with false information, malicious application, spam, fraud, phishing, click jacking and fake links, which lead to phishing attacks and etc. Therefore, we need to measure and improve the trust factor in the social networks.

Trust has been studied in many disciplines including sociology, psychology, and computer science. Each of these disciplines has defined and considered the trust from different perspectives; and their definitions may not be directly applicable to social networks (Sherchan, Nepal, & Paris, 2013). With the growth of social network services, the need for identifying trustworthy people has become a primary concern in order to protect users' vast amounts of information from being misused by unreliable users (Al-Oufi et al., 2012). It plays an important role in social networks and it is one of the biggest challenges of social networks (P. Manuel, 2013). In dictionaries, trust is generally related to "levels of confidence in something or someone" (Ko et al., 2011). In general, trust is a measure of confidence that an entity or entities will behave in an expected manner (Sherchan et al., 2013). Establishing trust among the indirectly connected users plays a pivotal role in improving the quality of social network services and enforcing the security for them (Jiang et al., 2014). It is the composition of multiple attributes such as reliability, honesty, truthfulness, dependability, security, competence, timeliness and Quality of Service (QoS) in the context of an environment (P. Manuel, 2013). Accordingly, identifying a trustworthy user to share information with, is a fundamental concern in social networks (Al-Oufi et al., 2012). Hence, we can view trust in the social networks as the users' level of confidence in using the social networks, and try to increase this by mitigating technical and psychological barriers for social networks services (Ko et al., 2011). Questions that appear are: how we can identify reliable users within the chain of connections and how we can prevent unreliable users from accessing the network and misusing information. To address these questions, ''trust'' is an invaluable notion in social network services that helps identify users to communicate and share information form with (Al-Oufi et al., 2012).

In spite of the importance of the trust evaluation in the social networks, evaluating the trust value based on QoS factors and call log history has not been investigated up to now. QoS is a set of nonfunctional properties that encompasses performance characteristics, such as execution cost, time, reliability and security (Chen, Paik, & Hung, 2013). Its requirements are evolving with the trustworthy computing (Jeong, 2013). On the other hand, call log was extracted from user relationships based on the extracted personal information (Kim & Park, 2013). A call log handled in this paper refers to interactions between the users in social networks. Therefore, it provides the valuable information to evaluate the trust between the users.

In this paper, we simplify trust model and derive a formula for the trust value in the social networks using call log histories and QoS requirements such as abundance, novelty, sincerity, accessibility, response ability, tendency to respond and agility. We mainly focus on trust in social networks where users can provide user-generated content and construct a list of trusted neighbors; and most importantly, the content is being classified as categories by design. This paper also describes how a service level agreement is prepared to combine the quality of service requirements of users. We propose the trust management approach by analyzing user behavioral patterns for social networks. For this purpose, we suggest a method to quantify a trusting relation based on the analysis of call log from social networks.

The rest of this paper is structured as follows: section 2 describes related works in social networks, section 3 discusses the proposed model, section 4 presents experimental results, section 5 maps out discussion and finally, section 6 concludes this paper.

2. Related Works

In this section, the state-of-the-art trust evaluation techniques in the social networks and their results are discussed and described.

Huang et al. (2010) have designed a model to find friends in the social network who share common interests. To compute trust values, they used a modified Dijkstra's algorithm along with the PageRank algorithm to calculate the popularity of a user in relation to a certain keyword. By combining the values inferred by the trust and popularity, the final ranked results of the search are generated.

Zolfaghar and Aghaie (2011) have moved toward time-aware trust prediction in evolving online trust networks. Achieving this, they investigated the impact of considering the temporal evolution of trust networks explicitly in trust prediction tasks using a supervised learning method. They incorporated the history information available on the trust relations (or links) of the current trust network state in the prediction process.

P. D. Manuel, Abd-El Barr, and Thamarai Selvi (2011) have proposed the trust model to evaluate the trust value based on the identity as well as behavioral trust. The proposed model applies the QoS metrics and increases the reliability as an important factor in trust.

Al-Oufi et al. (2012) have proposed the extended Advogato trust metric that facilitates the identification of trustworthy users associated with each individual user. By incorporating the strength of social relationships, they recursively diffused a capacity of a target user throughout his/her personal network. Also based on the capacity propagation they presented the capacity-first maximum flow method capable of finding the strongest path pertinent to discovering an ordered set of reliable users and preventing unreliable users from accessing personal networks.

Bravo, Squazzoni, and Boero (2012) have investigated the importance of the endogenous selection of partners for trust and cooperation in market exchange situations, where there is information asymmetry between investors and trustees. They created an experimental data-driven agent-based model where the endogenous link between interaction outcome and the social structure formation were examined starting from heterogeneous agent behavior. By testing various social structure configurations, they showed that dynamic networks lead to more cooperation when agents can create more links and reduce exploitation opportunities by free riders. Furthermore, they found that the endogenous network formation was more important for cooperation than the type of network.

Chen et al. (2013) have proposed a method to connect the isolated service islands into a global social service network to enhance the services' sociability on a global scale. First, they proposed linked social service-specific principles based on linked data principles for publishing services on the open Web as linked social services; then, they suggested a new framework for constructing the global social service network following linked social service-specific principles based on complex network theories. Next, an approach was proposed to enable the exploitation of the global social service network, providing linked social services as a service. Finally, experimental results showed that their approach can solve the quality of the service discovery problem, improving both the service discovering time and the success rate by exploring service-to-service based on the global social service network.

Jeong (2013) has proposed a QoS model for SaaS in enterprise resource planning. Using this QoS model, they proposed a multi-criteria decision-making system that finds the best fit for the SaaS in the Cloud computing environment and makes recommendations to users in priority order. In order to organize the quality clusters, they organized an expert group and got their opinion to organize the quality clusters using social network group. Social networks can be used efficiently to get an opinion from various types of expert groups. In order to establish the priority, they used pair wise comparisons to calculate the priority weights of each quality attribute, while accounting for their interrelation. Finally, using the quality network model and priority weights, this study evaluated three types of SaaS.

Deng, Huang, and Xu (2014a) have proposed a social network-based service recommendation method with trust enhancement known as "Relevant Trust Walker". First, a matrix factorization method was utilized to assess the degree of trust between users in a social network. Next, an extended random walk algorithm was proposed to obtain recommendation results.

Jiang et al. (2014) have focused on generating small trusted graphs for large social networks which can be used to make previous trust evaluation algorithms more efficient and practical. They showed how to preprocess a social network by developing a simple and practical userdomain-based trusted acquaintance chain discovery algorithm through using the small-world network characteristics of social networks and taking advantage of ‘‘weak ties’’. Then, they presented how to build a trust network and generate a trusted graph with the adjustable width breadth-first search algorithms.

Finally, Fan and Yeung (2015) have investigated the similarity level of community structures across different networks. They found the strong correlation with each other. Also they showed that the similarity between different networks may be helpful to find a community structure close to the underlying one. To verify this, they proposed a method to increase the weights of some connections in networks. With this method, new networks were generated to assist community detection. By doing this, the value of modularity can be improved and the new community structure matches the network’s natural structure better. Table 1 provides the side-by-side comparisons of the reviewed trust techniques in the social networks.

Table 1. The comparisons of the reviewed trust techniques in the social networks

#	Article	Approach	Results	Evaluation process
1	The similarity between community structures of different online social networks and its impact on underlying community detection (Fan & Yeung, 2015).	Proposing a method to increase some connections in the networks.	New networks are generated to assist community detection, the value of modularity can be improved and the new community structure matches network’s natural structure better.	Considering the Foursquare and Facebook applications as a social network group.
2	Social Network-based Service Recommendation with Trust Enhancement (Deng, Huang, & Xu, 2014b).	Proposing a social network-based service recommendation method with trust enhancement known as Relevant Trust Walker.	The quality of the recommendation and the speed of the method improved compared with existing algorithms.	Choosing Epinions as the data source for experiments.
3	A Novel Trust Management System for Cloud Computing- IaaS Providers (P. D. Manuel et al., 2011).	Proposing the trust model to evaluate the trust value of the based on the identity as well as behavioral trust.	Appling the QoS metrics and increases the reliability as an important factor in trust.	Simulating by varying the task number from 10 to 100 with different user requirements.

4	Generating trusted graphs for trust evaluation in online social networks (Jiang et al., 2014).	Generating small trusted graphs for large online social networks, which can be used to make previous trust evaluation algorithms more efficient and practical.	Focusing on generating small trusted graphs for large online social networks, and explores the stable and objective information for inferring trust.	Choosing Epinions as the data source for experiments.
5	Constructing a Global Social Service Network for Better Quality of Web Service Discovery (Chen et al., 2013).	Connecting the isolated service islands into a global social service network to enhance the services' sociability on a global scale.	Solving the quality of service discovery problem, improving both the service discovering time and the success rate by exploring service-to-service based on the global social service network.	Considering the Facebook application for experiments.
6	The QoS-based MCDM system for SaaS ERP applications with Social Network (Jeong, 2013).	Proposing a QoS model for SaaS in ERP.	Showing how to find the most suitable SaaS ERPs according to their correlation with the criteria and to recommend a SaaS ERP package which best suits users' needs.	Considering the Twitter application for experiments.
7	A group trust metric for identifying people of trust in online social networks (Al-Oufi et al., 2012).	Proposing the extended Advogato trust metric that facilitates the identification of trustworthy users associated with each individual user.	This approach has advantages over existing representative methods in terms of both the discovery of reliable users and the preventability of unreliable users.	Choosing Epinions as the data source for experiments.
8	Trust and partner selection in social networks: An experimentally grounded model (Bravo et al., 2012).	Investigating the importance of the endogenous selection of partners for trust	Results cast serious doubt about the static view of network structures on cooperation and can provides new insights into market efficiency.	Building an experiment Like model that exactly replicated the original experiment with calibrated parameters.

9	Evolution of trust networks in social web applications using supervised learning (Zolfaghar & Aghaie, 2011).	Proposing the time aware trust prediction model in evolving online trust networks.	Timestamps of past trust relations significantly improve the prediction accuracy of future trust Relations.	Choosing Epinions as the data source for experiments.
10	A novel social search model based on trust and popularity (Huang et al., 2010).	Proposing a model that is designed to find friends in an online social network who share common interests.	The model can provide more satisfactory searching results for users and provides wonderful support for friend searching and friend recommendation in OSNs.	Selecting "small-world" model as a simulation to realistic OSNs.

However, in spite of the importance of the call log histories and QoS factors in the social networks, evaluating the trust value based on them is not investigated up to now. Therefore, we present the proposed method based on QoS factors and call log histories.

3. Proposed Method

In this section, we propose a method to evaluate the trust values in the social networks based on QoS and call log. In section 3.1, the conceptual model of the proposed method will be described. Section 3.2 explains the QoS assurance technique. Next, in section 3.3, we present call log analyzer. Finally, section 3.4 discusses the trust evaluation mechanism.

3.1. Conceptual Model

The proposed approach to improve the trust evaluation mechanism in the social networks used two agents. In fact, it was built on users call log histories and QoS factors in social networks. The QoS factors consisting of the accessibility, response ability, tendency to respond and agility and call log histories consisting of the abundance, novelty, and sincerity. The main process of our approach is shown in Figure 1.

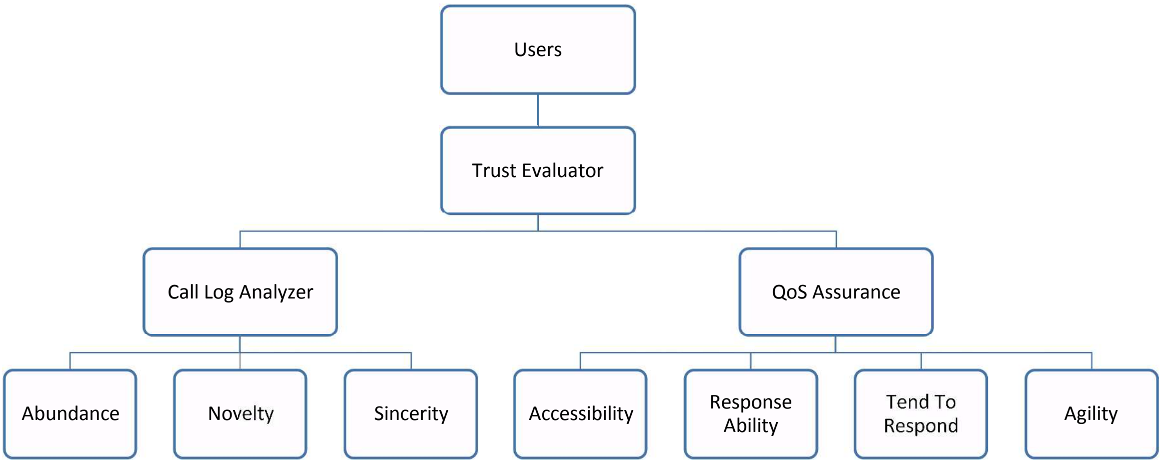

Fig.1.Conceptual model for the proposed trust evaluation method

3.2. QoS Assurance

We consider the credential attributes such as accessibility, response ability, tendency to respond, and agility to compute QoS assurance value that are described in this section.

3.2.1. Accessibility (AC)

Accessibility is a degree that shows a user is accessible when needed. The accessibility between user A and user B is computed through Eq. (1), where $Acc_{A,B}$ denotes the number of accepted requests from ‘A’ to ‘B’, $Rec_{A,B}$ denotes the total requests from ‘A’ to ‘B’. If the accessibility between ‘A’ and ‘B’ is greater than accessibility between ‘A’ and ‘C,’ it means that ‘A’ trusts to ‘B’ more than ‘C’.

$$AC_{A,B} = \frac{Acc_{A,B}}{Rec_{A,B}} \qquad (1)$$

3.2.2. Response Ability (RA)

Response Ability is the ability of a user to perform its required functions under stated conditions for a specified period. The response ability between user A and user B is computed through Eq. (2), where $Res_{A,B}$ denotes the number of requests from ‘A’ to ‘B’ that responded in the specified time, $Rec_{A,B}$ denotes the total requests from ‘A’ to ‘B’. If the response ability between ‘A’ and ‘B’ is less than the response ability between ‘A’ and ‘C,’ it means that ‘A’ trusts ‘C’ more than ‘B’.

$$RA_{A,B} = \frac{Res_{A,B}}{Rec_{A,B}} \qquad (2)$$

3.2.3. Tendency To Respond (TTR)

Tendency To Respond (TTR) is the number of logins whose messages the user trends to answer. TTR between user A and user B is computed through Eq. (3), where $Rl_{A,B}$ denotes the number of ‘A’ logins to response messages from ‘B’, $Tl_{A,B}$ denotes the total number of ‘A’ logins with requests from ‘B’. If tendency to respond between ‘A’ and ‘B’ is greater than that between ‘A’ and ‘C,’ it means that ‘A’ trusts ‘B’ more than ‘C’.

$$TTR_{A,B} = \frac{Rl_{A,B}}{Tl_{A,B}} \quad (3)$$

3.2.4. Agility (AG)

The actual response time is the exact time that 'B' responds 'A'. The expected response time is the expected time by 'A' to receive a response from 'B'. The agility between user A and user B is computed through Eq. (4), where $Ert_{A,B}$ denotes the expected time that 'B' responds to requests from 'A', $Art_{A,B}$ denotes the actual time that 'B' responds to requests from 'A'. If the agility between 'A' and 'B' is less than agility between 'A' and 'C,' it means that 'A' trusts 'C' more than 'B'.

$$AG_{A,B} = \frac{Ert_{A,B}}{Art_{A,B}} \quad (4)$$

3.3. Call Log Analyzer

User's relationships were quantified by analyzing call patterns based on abundance, novelty, and sincerity among users. Therefore, call log history analyzing phase includes these three important factors, which are described in this section.

3.3.1. Abundance (ABUN)

Abundance is the level of connections among the users. The abundance between user 'A' and user 'B' is computed through Eq. (5), where $Con_{A,B}$ denotes the total conversation between 'A' and 'B', $\sum_{k=1}^{n} Con_{A,B}$ denotes the total conversation that 'A' had with all other users. If the abundance between 'A' and 'B' is less than abundance between 'A' and 'C,' it means that 'A' talk with 'C' more than 'B', therefore, 'A' trusts 'C' more than 'B'.

$$\mathrm{ABUN}_{A,B} = \frac{Con_{A,B}}{\sum_{k=1}^{n} Con_{A,K}} \quad (5)$$

3.3.2. Novelty (NOV)

Novelty is the time flow of relationship among users. The novelty between user 'A' and user 'B' is computed through Eq. (6), where N denotes the total users, $Seq_{A,B}$ denotes the call recency between 'A' and 'B'. If the novelty between 'A' and 'C' is greater than novelty between 'A' and 'B', it means that 'A' talk with 'C' newly than 'B', therefore, 'A' trusts 'C' more than 'B'.

$$NOV_{A,B} = \frac{N - Seq_{A,B}}{\mathrm{N}} \quad (6)$$

3.3.3. Sincerity (SIN)

Sincerity is the duration of an inter-user relationship. The sincerity between user 'A' and user 'B' is computed through Eq. (7).

$$SIN_{A,B} = \alpha . Length\, S_{A,B} + (1- \alpha). LengthR_{B,A} \quad (7)$$

Send length ($Length\ S_{A,B}$) is computed through Eq. (8), where $L_{A,B}$ denotes the total call length between ‘A’ and ‘B’, $\sum_{k=1}^{n} L_{A,K} + \sum_{k=1}^{n} L_{K,A}$ denotes the total call length that ‘A’ had with all other users.

$$LengthS_{A,B} = \frac{L_{A,B}}{\sum_{k=1}^{n} L_{A,K} + \sum_{k=1}^{n} L_{K,A}} \tag{8}$$

On the contrary, received length ($Length\ R_{A,B}$) is computed through Eq. (9), where $L_{B,A}$ denotes the total call length between ‘B’ and ‘A’, $\sum_{k=1}^{n} L_{A,K} + \sum_{k=1}^{n} L_{K,A}$ denotes the total call length that ‘A’ had with all other users.

$$Length\ R_{A,B} = \frac{L_{B,A}}{\sum_{k=1}^{n} L_{A,K} + \sum_{k=1}^{n} L_{K,A}} \tag{9}$$

The α value is applied after dividing $Length\ S_{A,B}$ and $Length\ R_{A,B}$ to show the weighted value of the send through Eq. (10), where $Length\ S_{A,B}$ denotes the send length between user ‘A’ and user ‘B’ and $Length\ R_{A,B}$denotes the received length between user ‘A’ and user ‘B’.

$$\alpha_{A,B} = \frac{Length\ R_{A,B}}{Length\ S_{A,B}} \tag{10}$$

3.4. Trust Evaluation

In this section, we propose a trust evaluation mechanism and derive a formula for it using the call log and QoS requirements. Where $ABUN_{A,B}$ denotes the abundance value between user ‘A’ and user ‘B’, $NOV_{A,B}$ denotes the novelty value between user ‘A’ and user ‘B’. ; $SIN_{A,B}$ denotes the sincerity value between user ‘A’ and user ‘B’; $AC_{A,B}$ denotes the accessibility value between user ‘A’ and user ‘B’; $RA_{A,B}$ denotes the response ability value between user ‘A’ and user ‘B’; $TTR_{A,B}$ denotes the tendency to respond value between user ‘A’ and user ‘B’ and $AG_{A,B}$ denotes the agility value between user ‘A’ and user ‘B’. So, trust can be obtained through synthesis of abundance, novelty, sincerity, accessibility, response ability, tend to respond and agility. The trust between user A and user B is computed through Eq. (11).

$$\mathrm{T}_{A,B} = W_1.\mathrm{ABUN}_{A,B} + W_2.\mathrm{NOV}_{A,B} + W_3.SIN_{A,B} + W_4.AC_{A,B} + W_5.RA_{A,B} + W_6.TTR_{A,B} + W_7.AG_{A,B} \tag{11}$$

The synthesis of these seven factors ranges from ‘0’ to ‘1’ in real number. Where w1, w2, w3, w4, w5, w6 and w7 are positive weights of the trust parameters such that w1 + w2 + w3 + w4 + w5 + w6+w7 = 1. The weights of the trust attributes are predetermined based on their priority. For example, w1 = 0.0052, w2 = 0.1459, w3 = 0.0702, w4 = 0.3437, w5 = 0.1347, w6 = 0.2287, w7 = 0.0717. In this example, accessibility is given the maximum priority while abundance is given the minimum priority. The variables for proposed trust evaluation method are shown in table 2.

Table 2. Variables for proposed trust evaluation method

Variables	Description
$ACC_{A,B}$	Number of accepted requests from A to B
$REC_{A,B}$	Total request from A to B

$RES_{A,B}$	Number of requests from A to B that responded
$RL_{A,B}$	Number of A logins to response a message from B
$TL_{A,B}$	Total number of logins with requests from B
$ERT_{A,B}$	Expected time that B response to A requests
$ART_{A,B}$	Actual time that B response to A requests
$CON_{A,B}$	Total conversation between A and B
$SEQ_{A,B}$	Call recency between A and B
$L_{A,B}$	Total call length between A and B

3.5. Algorithm of Trust Evaluation

Step 1: Create relational data of users.
Step 2: Get a list of friends for each user.
Steps 3 and 4: Get the number of user conversation and calculate the abundance of the user.
Steps 5 and 6: Get the sequence of user conversation and calculate novelty of user.
Step 7: Check if the user has any received message.
Steps 8 and 9: Get the length of send, receive a message, and calculate sincerity of user.
Step 10: Check if the user accepts any received message.
Step 11: Calculate accessibility.
Step 12: Check if a user logged in.
Step 13: Check if user response any received the message.
Steps 14 and 15: Calculate response ability and calculate tend to respond.
Steps 16 and 17: Get the weights for parameters and calculate trust value.
Step 18: Get the set of untrusted users.
Step 19 Get the set of trusted users.
Step 20: Get the top-n users.
Steps 21, 22, and 23: Calculate error-hit, recall, and precision.

4. Experimental Results

In this section, in order to test the performance of the proposed method, we use a standard evaluation technique in the social networks. Therefore, we consider whether our approach improves the prison of trust evaluator in the social networks or not. Hence, in section 4.1, we present simulation environment. Next, in section 4.2, we introduce the simulation parameters. Finally, in section 4.3, we present the obtained results.

4.1. Simulation Environment

The simulation is performed using CPU core i7, memory 8GByte DDR3L, and 8MByte cache memory. The experiments have been obtained with a system simulator programmed in Matlab R2013b and user's data was extracted from our random dataset.

4.2. Simulation Parameters

In this work, we mainly focus on the friendship of users in social networks. People may register on social networks to keep in touch with friends. Social networks managers are aware of an issue that user's data are their validity. Therefore, we should not expect that they share these data. Therefore, due to the social networks, databases are almost private, and our parameters do not exist in the available datasets, so we create a dataset to show the relation between the users. After preparing the dataset, we enter the modeling phase. We calculate the value of abundance, novelty, sincerity, accessibility, response ability, tendency to respond, and agility. Their average value is between zero and one. To evaluate the accuracy of the proposed method, experiments on a dataset were conducted. Since the user's data and information in the social networks are private and we cannot have access to it, in constructing a new data set for the present study, we create random data to calculate abundance, novelty, sincerity, accessibility, response ability, tendency to respond and agility. For evaluation purpose, we consider uniform distribution (it is a distribution that has constant probability), Poisson distribution (a discrete frequency distribution which gives the probability of a number of independent events occurring in a fixed time) and exponential distribution (a process in which events occur continuously and independently at a constant average rate). In addition, we assumed 2000 users in a social network. The number of calls among users was between 1 and 10000. In addition, the call sequence among users was between 1 and 100. Moreover, the number of input calls accepted and responded by the users was between 100 and 500. The rest of the experiment setting for simulation parameters are shown in table 3.

Table 3. Experiment setting for simulations

Experiment variables	Value (range)	Distribution
The number of users		Uniform
The number of calls among users	2000	Poisson
The call sequence among the users	1 ~ 10000	Exponential
The call length between the users	1 ~ 100	Exponential
The total number of input calls of users	1500 ~ 10500	Poisson
The number of input calls accepted by the users	500 ~ 1000	Poisson
The number of input calls responded by the	100 ~ 500	Poisson
users	100 ~ 500	Poisson
the number of user logins to response messages	0 ~ 200	Poisson
The total number of user logins	200 ~ 500	Exponential
The expected response time by the users	750 ~ 2000	Exponential
(second)	1000 ~ 6300	
The actual response time by the users (second)		

4.3. Obtained Results

In this section, we conduct several experiments to compare our approach with other methods. Therefore, we present experimental results that show the effects of the parameter adjustments. The experiments are conducted in two phases. In the first phase, we evaluate the trust value based on combined model, FIFO, call log histories and QoS. In the second phase, we use error-hit, precision and recall to measure the accuracy of the trustworthy user identification and test the performance of the proposed method. Moreover, error-hit, precision, and recall comparison results can show the effectiveness of proposed method. Finally, we compare our approach trust value with other state-of-the-art methods.

Error-hit measures how often the approach includes untrustworthy users in a list of trusted users. The error-hit value is computed through Eq. (12) (Al-Oufi et al., 2012), where $Trust^{-}$ shows the set of untrusted users, Top is a top-n identified users and K denotes the number of users.

$$Error\ Hit = \frac{1}{K}\sum_{s=1}^{k}\frac{Trust^{-} \cap Top}{Top} \tag{12}$$

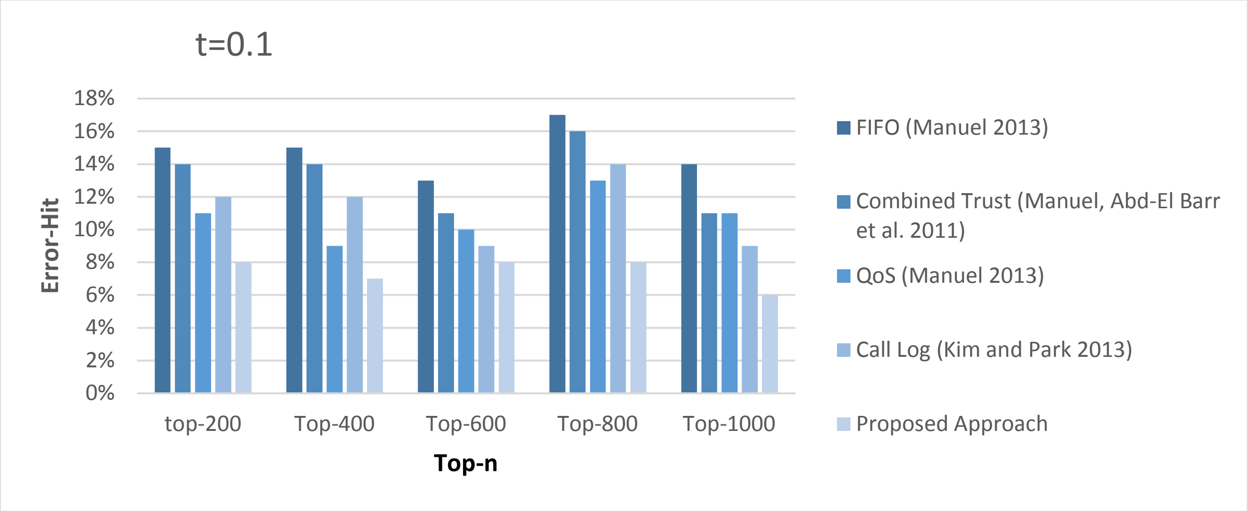

Fig.3.comparativeresults of error-hit at threshold = 0.1

Fig. 3 depicts error-hit at threshold = 0.1 according to top-n users. As a result, we observed that from top-200 to top-1000, the error-hit of proposed approach is less than call log, QoS, FIFO and combined trust model. It means that the other models include untrustworthy users more than proposed approach.

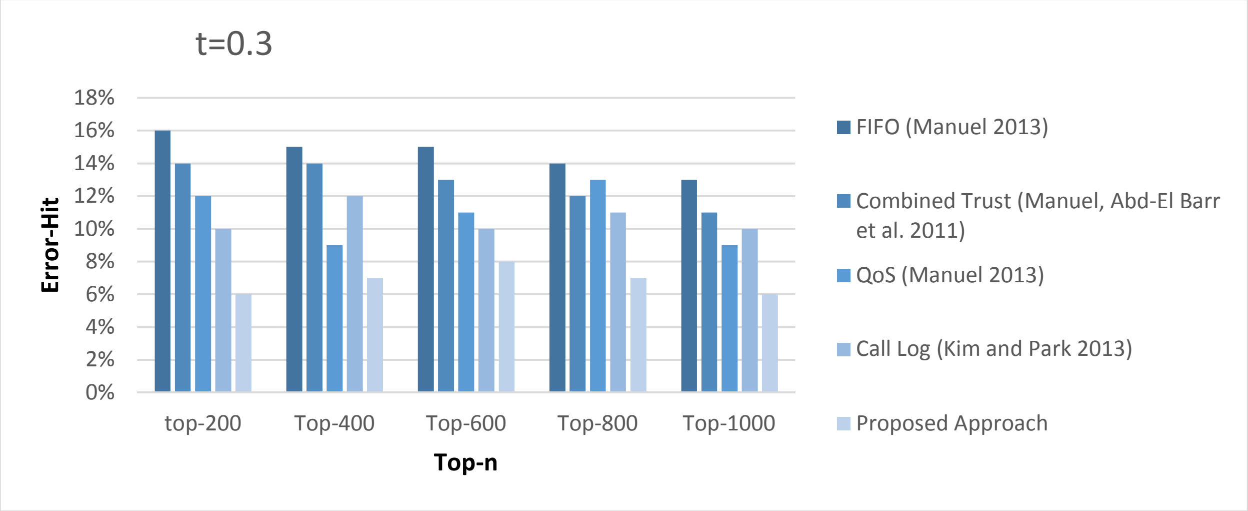

Fig.4.comparativeresults of error-hit at threshold = 0.3

Fig. 4 depicts error-hit at threshold = 0.3 according to top-n users. As a result, we observed that from top-200 to top-1000, the error-hit of proposed approach is less than call log, QoS, FIFO and combined trust model. It means that the other models include untrustworthy users more than proposed approach.

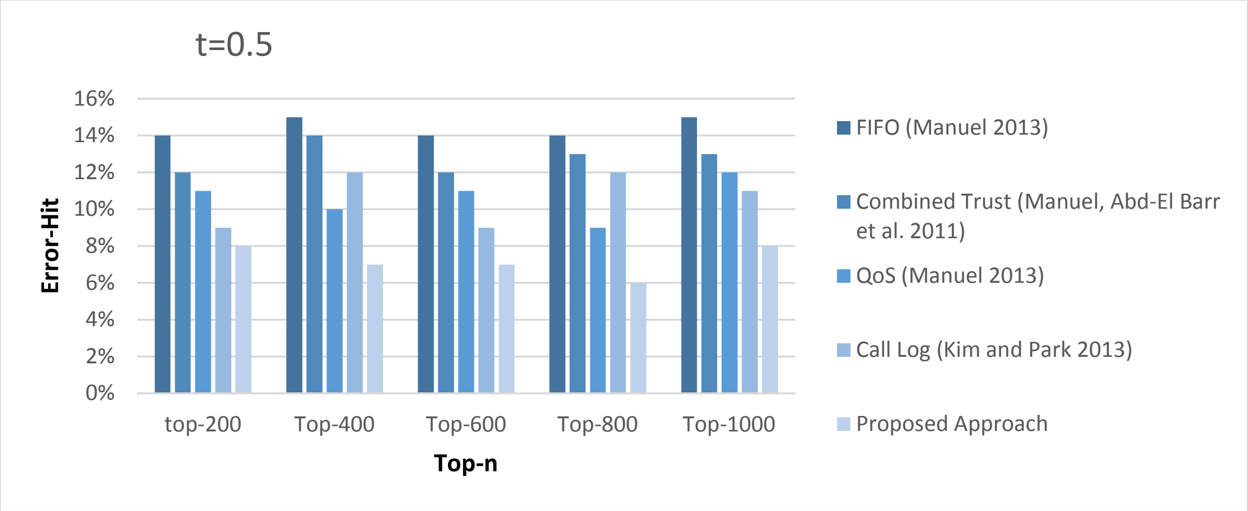

Fig.5.comparativeresults of error-hit at threshold = 0.5

Fig. 5 depicts error-hit at threshold = 0.5 according to top-n users. As a result, we observed that from top-200 to top-1000, the error-hit of proposed approach is less than call log, QoS, FIFO and combined trust model. It means that the other models include untrustworthy users more than proposed approach.

Recall measures how potentially the approach prevents unreliable users from accessing individual users. The recall value is computed through Eq. (13) (Al-Oufi et al., 2012), where $Trust^{+}$ shows the set of trusted users, Top is a top-n identified users and K denotes the number of users.

$$Recall = \frac{1}{K}\sum_{s=1}^{k}\frac{Trust^{+}\ \cap Top}{Trust^{+}} \tag{13}$$

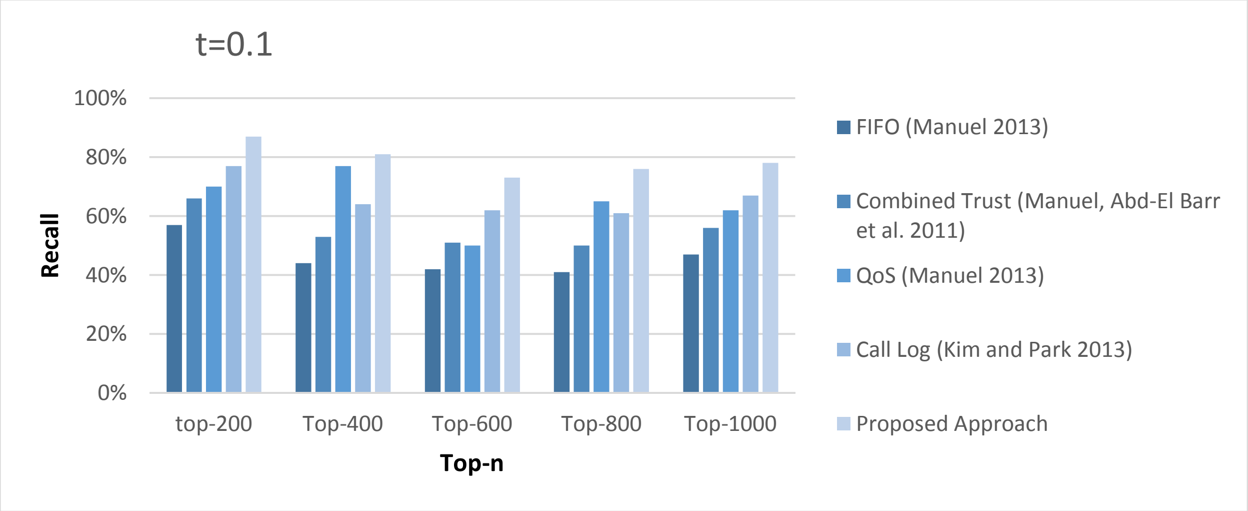

Fig.6.comparativeresults of recall at threshold = 0.1

Fig. 6 depicts recall at threshold = 0.1 according to top-n users. As a result, we observed that from top-200 to top-1000, the recall of proposed approach is more than call log, QoS, FIFO and combined trust model. It means that the proposed approach prevents unreliable users from accessing individual users more than other models.

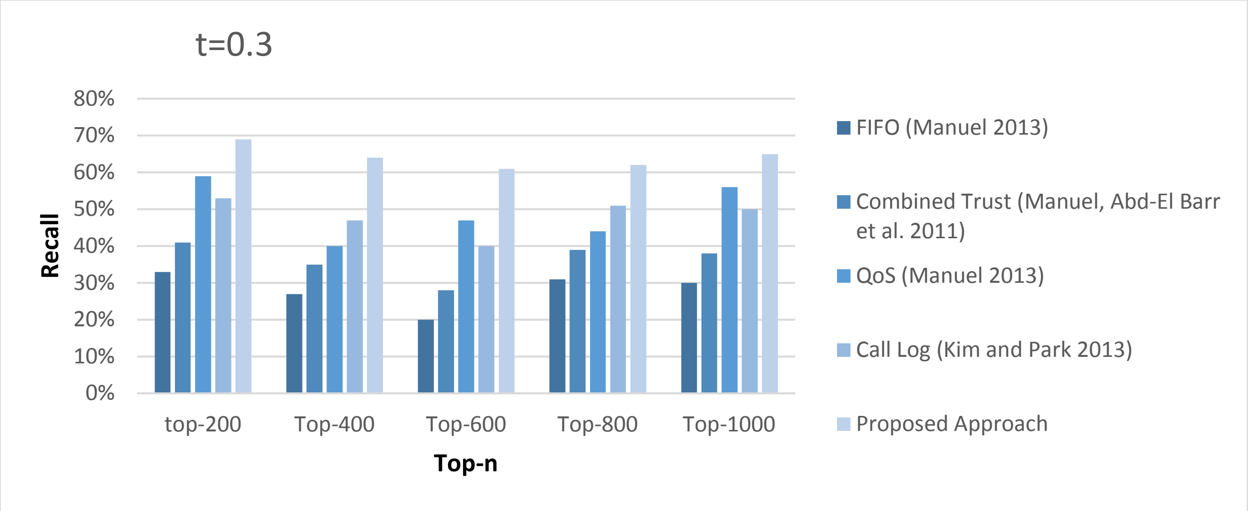

Fig.7.comparativeresults of recall at threshold = 0.3

Fig. 7 depicts recall at threshold = 0.3 according to top-n users. As a result, we observed that from top-200 to top-1000, the recall of proposed approach is more than call log, QoS, FIFO and combined trust model. It means that the proposed approach prevents unreliable users from accessing individual users more than other models.

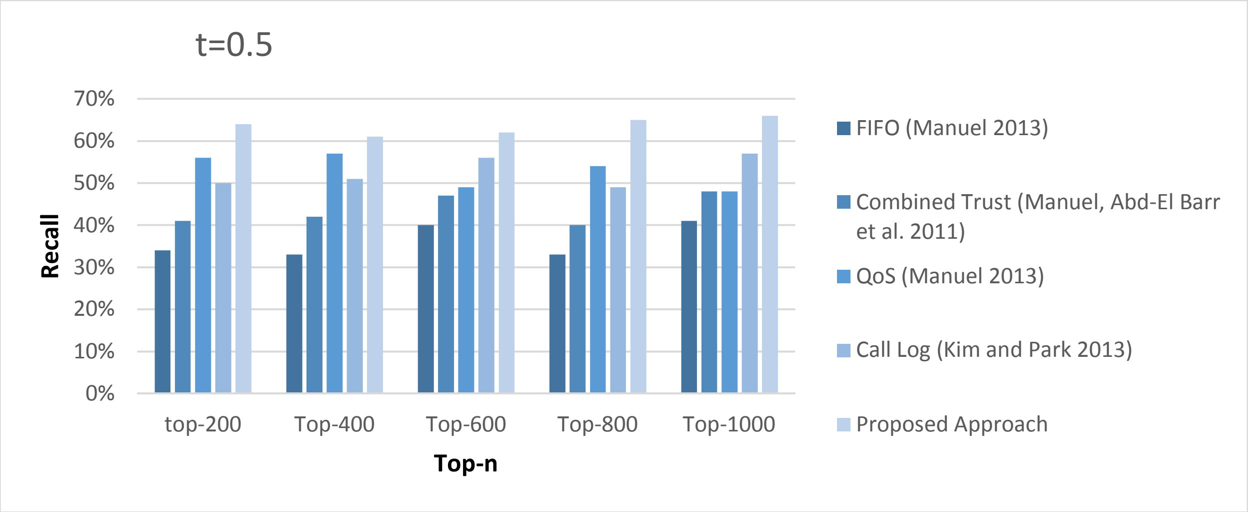

Fig.8.comparativeresults of recall at threshold = 0.5

Fig. 8 depicts recall at threshold = 0.5 according to top-n users. As a result, we observed that from top-200 to top-1000, the recall of proposed approach is more than call log, QoS, FIFO and combined trust model. It means that the proposed approach prevents unreliable users from accessing individual users more than other models.

Precision measures how well the approach identifies a group of trust about individual users. The precision value is computed through Eq. (14) (Al-Oufi et al., 2012), where $Trust^{+}$ shows the set of trusted users, Top is a top-n identified users and K denotes the number of users.

$$Precision = \frac{1}{K}\sum_{s=1}^{k}\frac{Trust^{+}\ \cap Top}{Top} \tag{14}$$

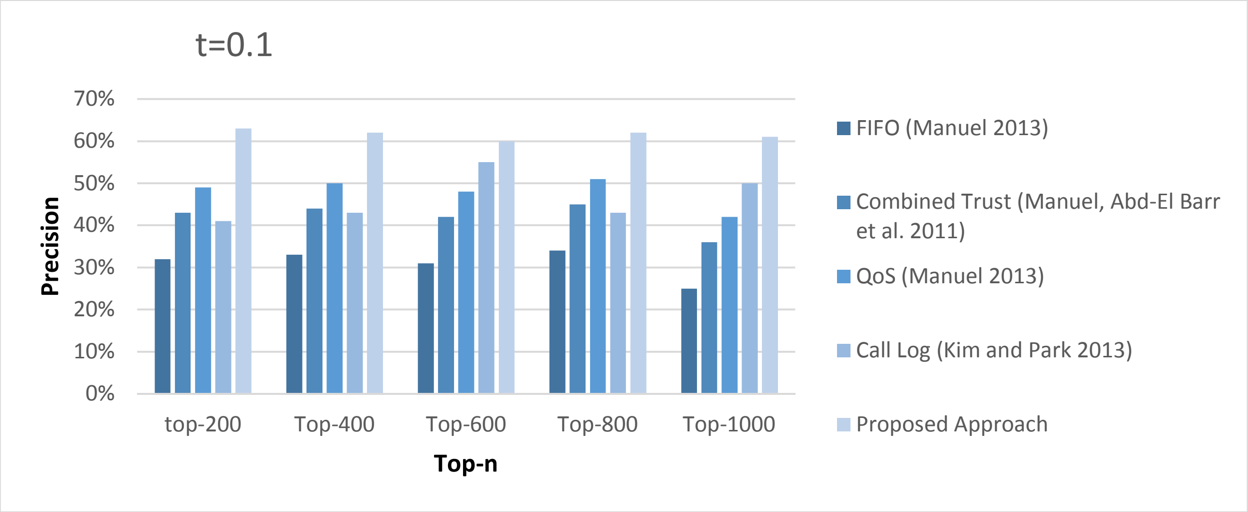

Fig.9.comparativeresults of precision at threshold = 0.1

Fig. 9 depicts precision at threshold = 0.1 according to top-n users. As a result, we observed that from top-200 to top-1000, the precision of proposed approach is more than call log, QoS, FIFO and combined trust model. It means that the proposed approach identifies a group of trust about individual users more than other models.

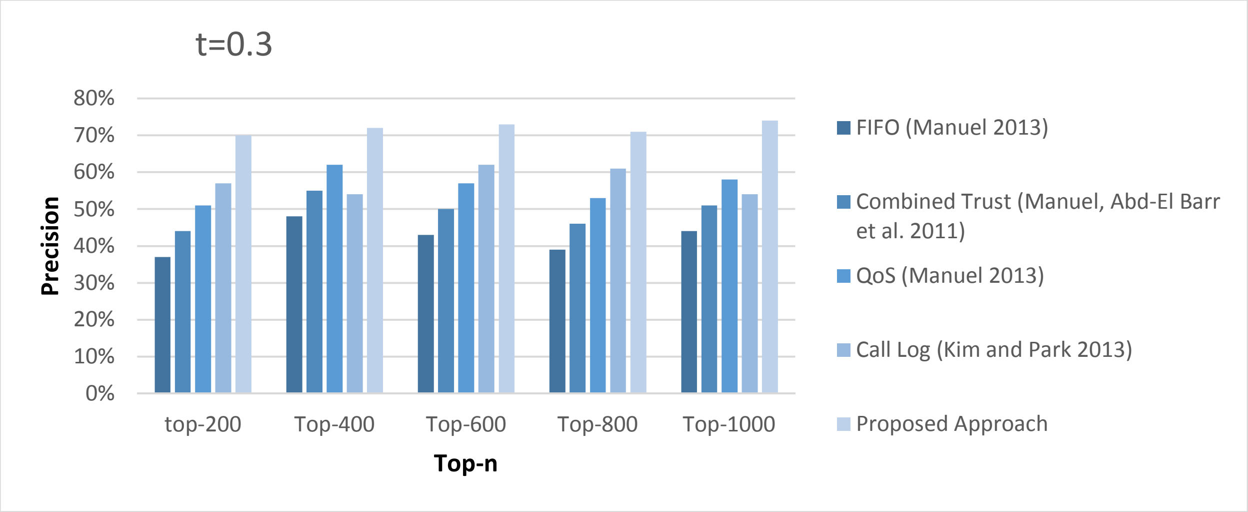

Fig.10.comparativeresults of precision at threshold = 0.3

Fig. 10 depicts precision at threshold = 0.3 according to top-n users. As a result, we observed that from top-200 to top-1000, the precision of proposed approach is more than call log, QoS, FIFO and combined trust model. It means that the proposed approach identifies a group of trust about individual users more than other models.

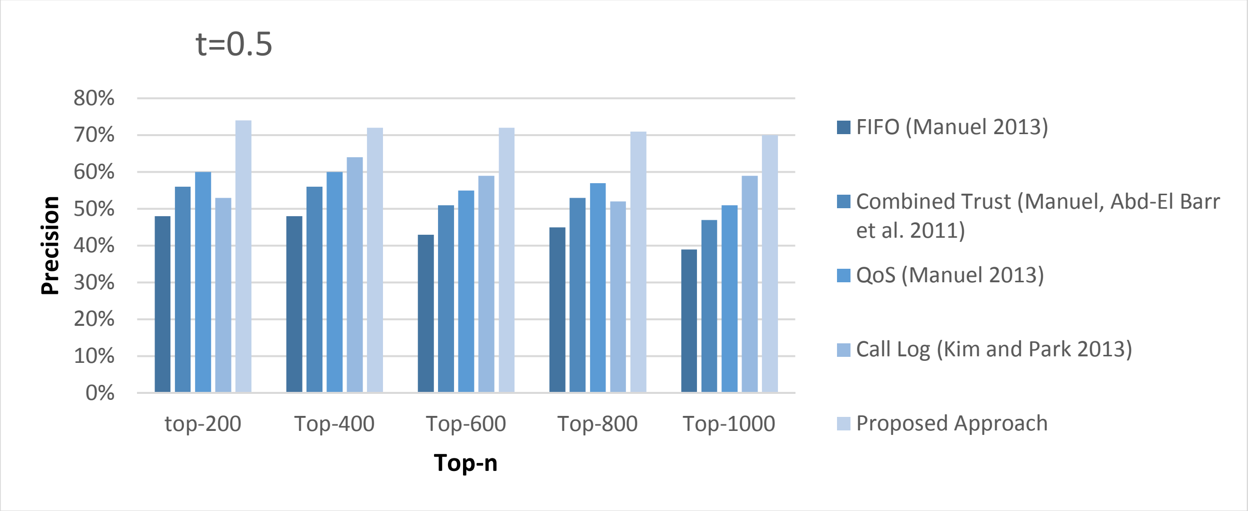

Fig.11.comparativeresults of precision at threshold = 0.5

Fig. 11 depicts precision at threshold = 0.5 according to top-n users. As a result, we observed that from top-200 to top-1000, the precision of proposed approach is more than call log, QoS, FIFO and combined trust model. It means that the proposed approach identifies a group of trust about individual users more than other models.

As a result, error-hit, precision, and recall comparison results can show the effectiveness of the proposed method. The evaluation results show that the proposed method can be applied directly to the existing social networks and provide high recommendation accuracy. This fact can be helpful in trust prediction for large datasets.

5. Discussion

In this paper, we presented the trust model and derived a formula for trust value in the social networks using call log histories and QoS requirements such as abundance, novelty, sincerity, accessibility, response ability, tendency to respond, and agility. The obtained results showed that the proposed approach improves the error-hit, precision and recall over call log, QoS, FIFO and combined trust model. Therefore, it also improves the trust value.

In spite of the importance of call log and QoS in the social networks, there are only a few papers that focus on this issue. For example, Chen et al. (2013) have considered trust and QoS, Donner (2006) has considered trust and call log, Jeong (2013) has considered trust and QoS, Zuluaga (2013) has considered trust and QoS, Balasubramaniyan, Ahamad, and Park (2007) have considered trust and call log and Deng et al. (2014a) have considered trust and QoS. Therefore, in this paper, we provide a method to evaluate trust in social networks using call log histories and QoS. We compare the proposed approach with other methods in these terms. The comparison between the related works is shown in table 4.

Table 4. The comparisons between related works

Mechanism	Trust	Call Log	QoS
Proposed Approach	✓	✓	✓
Chen et al. (2013)	✓	×	✓
Jeong (2013)	✓	×	✓
Donner (2006)	✓	✓	×
Zuluaga (2013)	✓	×	✓
Balasubramaniyan et al. (2007)	✓	✓	×
Deng et al. (2014a)	✓	×	✓

6. Conclusion and future work

This paper presents a trust evaluating method based on call log histories and QoS requirements. We extended the proposed trust model in ways that can be incorporated with the strength of social relationships and discovered a group of reliable users associated with each individual user. Such an underlying community structure can help analyze people's behaviors and the relationships among them. To achieve that, we first studied the relations in different social networks. By combining call log and QoS, a trust value is modeled. This paper has four main goals: 1) evaluating the trust value, 2) calculating error-hit in order to measure how often the approach includes untrustworthy users in a list of trusted users, 3) calculating precision in order to measure how well the approach identifies a group of trust with regard to individual users, 4) calculating recall in order to measure how the approach potentially prevents unreliable users from accessing individual users.

The experimental results demonstrated that the proposed model performs better than the call log, QoS, FIFO model and combined trust model. We show that the proposed model error-hit, precision, and recall are better than the other four models. Here, trust is measured in terms of seven attributes. However, there are some more attributes such as honesty, similarity of user profiles, and users' activity based community discovery. These parameters have not been discussed here. Therefore, we plan to refine trust using these additional attributes in our future work.

References

Al-Oufi, S., Kim, H.-N., & El Saddik, A. (2012). A group trust metric for identifying people of trust in online social networks. *Expert Systems with Applications, 39*(18), 13173-13181.

Ashouraie, M., & Jafari Navimipour, N. (2015). Priority-based task scheduling on heterogeneous resources in the Expert Cloud. *Kybernetes, 44*(10), 1455-1471.

Balasubramaniyan, V., Ahamad, M., & Park, H. (2007). *CallRank: Combating SPIT Using Call Duration, Social Networks and Global Reputation.* Paper presented at the CEAS.

Bravo, G., Squazzoni, F., & Boero, R. (2012). Trust and partner selection in social networks: An experimentally grounded model. *Social Networks, 34*(4), 481-492.

Charband, Y., & Navimipour, N. J. (2016). Online knowledge sharing mechanisms: a systematic review of the state of the art literature and recommendations for future research. *Information Systems Frontiers*, 1-21.

Chen, W., Paik, I., & Hung, P. (2013). Constructing a global social service network for better quality of web service discovery.

Chiregi, M., & Jafari Navimipour, N. (2016). Trusted services identification in the cloud environment using the topological metrics. *Karbala International Journal of Modern Science*.

Deng, S., Huang, L., & Xu, G. (2014a). Social Network-based Service Recommendation with Trust Enhancement. *Expert Systems with Applications*.

Deng, S., Huang, L., & Xu, G. (2014b). Social network-based service recommendation with trust enhancement. *Expert Systems with Applications, 41*(18), 8075-8084.

Donner, J. (2006). The use of mobile phones by microentrepreneurs in Kigali, Rwanda: Changes to social and business networks. *Information Technologies & International Development, 3*(2), pp. 3-19.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 Proceedings*, 339.

Fan, W., & Yeung, K. (2015). Similarity between community structures of different online social networks and its impact on underlying community detection. *Communications in Nonlinear Science and Numerical Simulation, 20*(3), 1015-1025.

Hazratzadeh, S., & Jafari Navimipour, N. (2017). Colleague recommender system in the Expert Cloud using the features matrix. *Kybernetes*.

Huang, C., Chen, Y., Wang, W., Cui, Y., Wang, H., & Du, N. (2010). *A novel social search model based on trust and popularity.* Paper presented at the Broadband Network and Multimedia Technology (IC-BNMT), 2010 3rd IEEE International Conference on.

Jafari Navimipour, N., & Charband, Y. (2016). Knowledge sharing mechanisms and techniques in project teams: literature review, classification, and current trends. *Computers in Human Behavior*.

Jafari Navimipour, N., Masoud Rahmani, A., Habibizad Navin, A., & Hosseinzadeh, M. (2014). Job scheduling in the Expert Cloud based on genetic algorithms. *Kybernetes, 43*(8), 1262-1275.

Jafari Navimipour, N., Rahmani, A. M., Habibizad Navin, A., & Hosseinzadeh, M. (2015). Expert Cloud: A Cloud-based framework to share the knowledge and skills of human resources. *Computers in Human Behavior, 46*(C), 57-74.

Jeong, H.-Y. (2013). The QoS-based MCDM system for SaaS ERP applications with Social Network. *The Journal of Supercomputing, 66*(2), 614-632.

Jiang, W., Wang, G., & Wu, J. (2014). Generating trusted graphs for trust evaluation in online social networks. *Future generation computer systems, 31*, 48-58.

Kim, M., & Park, S. O. (2013). Trust management on user behavioral patterns for a mobile cloud computing. *Cluster computing, 16*(4), 725-731.

Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). *TrustCloud: A framework for accountability and trust in cloud computing.* Paper presented at the Services (SERVICES), 2011 IEEE World Congress on.

Manuel, P. (2013). A trust model of cloud computing based on Quality of Service. *Annals of Operations Research*, 1-12.

Manuel, P. D., Abd-El Barr, M. I., & Thamarai Selvi, S. (2011). A Novel Trust Management System for Cloud Computing IaaS Providers. *JCMCC-Journal of Combinatorial Mathematicsand Combinatorial Computing, 79*, 3.

Navimipour, N. J. (2015a). A formal approach for the specification and verification of a Trustworthy Human Resource Discovery mechanism in the Expert Cloud. *Expert Systems with Applications, 42*(15), 6112-6131.

Navimipour, N. J. (2015b). Task scheduling in the Cloud Environments based on an Artificial Bee Colony Algorithm.

Navimipour, N. J., & Khanli, L. M. (2008). *The LGR method for task scheduling in computational grid.* Paper presented at the Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on.

Navimipour, N. J., & Milani, F. S. (2014). A comprehensive study of the resource discovery techniques in Peer-to-Peer networks. *Peer-to-Peer Networking and Applications, 8*(3), 474-492.

Navimipour, N. J., & Milani, F. S. (2015). Task scheduling in the cloud computing based on the cuckoo search algorithm. *International Journal of Modeling and Optimization, 5*(1), 44.

Navimipour, N. J., Rahmani, A. M., Navin, A. H., & Hosseinzadeh, M. (2015). Expert Cloud: A Cloud-based framework to share the knowledge and skills of human resources. *Computers in Human Behavior, 46*, 57-74.

Navimipour, N. J., & Soltani, Z. (2016). The impact of cost, technology acceptance and employees' satisfaction on the effectiveness of the electronic customer relationship management systems. *Computers in Human Behavior, 55*, 1052-1066.

Navimipour, N. J., & Zareie, B. (2015). A model for assessing the impact of e-learning systems on employees' satisfaction. *Computers in Human Behavior, 53*, 475-485.

Navin, A. H., Navimipour, N. J., Rahmani, A. M., & Hosseinzadeh, M. (2014). Expert grid: new type of grid to manage the human resources and study the effectiveness of its task scheduler. *Arabian Journal for Science and Engineering, 39*(8), 6175-6188.

Sharif, S. H., Mahmazi, S., Navimipour, N. J., & Aghdam, B. F. (2013). A review on search and discovery mechanisms in social networks. *International Journal of Information Engineering & Electronic Business, 5*(6).

Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys (CSUR), 45*(4), 47.

Soltani, Z., & Navimipour, N. J. (2016). Customer relationship management mechanisms: A systematic review of the state of the art literature and recommendations for future research. *Computers in Human Behavior, 61*, 667-688.

Souri, A., & Navimipour, N. J. (2014). Behavioral modeling and formal verification of a resource discovery approach in Grid computing. *Expert Systems with Applications, 41*(8), 3831-3849.

Zareie, B., & Jafari Navimipour, N. (2016). The Effect of Electronic Learning Systems on the Employee's Commitment. *The International Journal of Management Education*.

Zareie, B., & Navimipour, N. J. (2016). The impact of electronic environmental knowledge on the environmental behaviors of people. *Computers in Human Behavior, 59*, 1-8.

Zolfaghar, K., & Aghaie, A. (2011). Evolution of trust networks in social web applications using supervised learning. *Procedia Computer Science, 3*, 833-839.

Zuluaga, B. (2013). Quality of social networks and educational investment decisions. *The Journal of Socio*-Economics, 43, 72-82.