Trust Evaluation in Social Networking: A Review

Sihui Zhao
State Key Laboratory on Integrated Services Networks
Xidian University
Xi'an, China
(86) 13149245226
zhaosihui615@163.com

Zheng Yan
State Key Laboratory on Integrated Services Networks
Xidian University, Xi'an, China
Department of Comnet
Aalto University, Espoo, Finland
zyan@xidian.edu.cn

ABSTRACT
Social networking has become very popular in recent years by serving as a medium for disseminating information and connecting like-minded people. It influences today's social culture and changes the way of modern life. The success of social networking relies on the level of trust that social group members have with each other as well as with social networking service providers. Therefore, trust evaluation in the social networking becomes an important topic that has attracted special concerns. Many trust models or schemes have been proposed to improve the security or performance in social networking. However, existing work mostly only focused on certain aspects. There still lacks a comprehensive study on trust evaluation and management in social networking. In this paper, we propose comprehensive criteria with nine aspects for trust evaluation. Related work in this area published in recent five years have been seriously surveyed and evaluated based on the criteria. We compare existing work and analyze the advantages and disadvantages of the current methods in order to figure out open research issues and motivate future research efforts.

CCS Concepts
• General and reference→Surveys and overviews • General and reference→Evaluation

Keywords
Trust evaluation, social networking, reputation management

1. INTRODUCTION
Social networking originates from the gam in networks, and the starting point of the latter is Email. In the Email era, the Internet can only satisfied 5% of the needs of human social interactions. However, in today's rich social networks, that figure could have been raised at least 10 times [14]. Nowadays, the social networking plays an important role in people's life, and has far-reaching effects on people's access to information, thinking and living.

The social networking is more than a platform for users to show themselves, make friends, and disseminate information. It plays an important role as indispensable tools for professional networking, social recommendations, advertisement, and so many. But today's social networking still has some drawbacks, e.g., disclosure of personal information and dissemination of fake information. In order to safeguard the privacy concerns of users and the open nature of the Internet, people proposed using a trust evaluation model to help users distinguish the dishonest information that cannot be trusted in the social networking.

Trust plays a key role in social networking. However it is calculative, emotional, cognitive, institutional and relational, thus hard to evaluate. It represents the perceived sense of reliability by each individual associated with each interaction that is often based on past experiences. In different kinds of trust evaluation models, trust information collection and trust value assessments are diverse. The goal of this paper is to propose uniform criteria to assess the trust evaluation models proposed in recent years. The purpose of this review is to comment current research problems in this research field and propose future research directions.

The rest of the paper is organized as follows. In Section 2, we describe the basic concepts related to our review and introduce the criteria used for assessing the performance of trust evaluation in the social networking. Then we present an overview of the literature about trust evaluation in the social networking by measuring each work with the criteria in Section 3. In Section 4, we discuss the problems of current research and propose future research directions. Finally, conclusion is presented in the last section.

2. BASIC CONCEPS AND CRITERIA

2.1 Basic Concepts.

2.1.1 Definition 1: trust
Trust has been defined in many disciplines, such as sociology, psychology, computer science, etc. In psychology, trust is considered to be a psychological state of an individual, who risks being vulnerable to a trustee based on positive expectations of the trustee's intentions or behaviors. In sociology, trust is defined as "a bet about the future contingent actions of the trustee". However, we take the natural definition of ''trust'', that is, Golbeck's definition in the context of a social web where ''trust in a person is a commitment to an action based on a belief that the future actions of that person will lead to a good outcome'' [1]. In general, trust is the confidence that other people or systems can be relied on.

2.1.2 Definition 2: trust model
The method to specify, evaluate, set up, and ensure trust relationships

MOBIMEDIA 2016, June 18-19, Xi'an, People's Republic of China

DOI 10.4108/eai.18-6-2016.2264178

among entities is the trust model [19]. Trust model aims to solve the following problems:

- How to determine the certificate that can prove that an entity is trusted?
- How to build up a trust relationship?
- How to limit and control the trust relationship under certain circumstances?

Trust model generally performs the function of trust derivation, computation, and application. During trust computation, it needs to estimate the overall trust in an entity according to trust factors.

2.1.3 Definition 3: social networking

Barnes first introduced the concept of social networking in 1954. He described it as connected graphs where nodes represent entities and edges their interdependencies [12]. Entities are a set of social actors such as individuals, organizations and groups. The edges could be interactions, invitations, trades, etc. Figure 1 shows an example of social networking, looking from a specific person: Alice. The nodes represent people and the edges are relationships amongst them. This specific network depicts Alice's relationships with different people.

From another perspective, the social networking is the use of internet-based social media programs to make connections with friends, family, classmates, customers and clients. The social networking can be established for social purposes, business purposes or both. Examples of the social networking include Facebook, LinkedIn and WeChat, all of which are very popular and widely used all over the world.

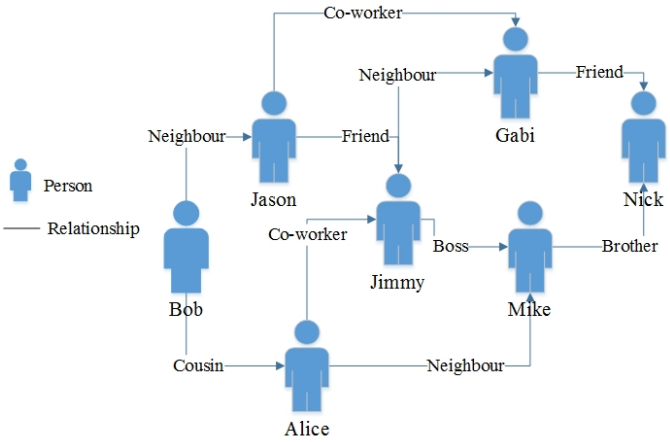

Figure 1. An example of social networking

2.2 Criteria on Trust Evaluation in Social Networking

We propose uniform review criteria on trust evaluation for assessing its performance. In our opinion, a comprehensive and holistic trust evaluation in social networking requires to achieve all the following objectives.

- Trustworthiness (T): the trust model is robust to overcome various potential attacks，such as dishonest votes, social bot attacks, orchestrated attacks and so on.
- Adaptability (Ad): The trust model in social networking is adaptive to context changes with dynamic support.
- Usability (Us): The trust model considers trustor's subjective opinion and is usable with regard to user-device interaction.
- Privacy (Pr): User privacy is preserved when user data are collected for trust evaluation, which greatly encourage social networking data sharing.
- Accuracy (Ac): the trust model is accurate in terms of trust/reputation evaluation.
- Efficiency (E): the trust model is efficient to dynamically manage trust relationships.
- Uniformity (Un): the trust model can unify user votes with trustworthy credibility.
- Comprehension (C): the trust model supports various trust influencing factors. There are many subjective and objective impact factors that should be considered in reputation and trust evaluation. The more comprehensive a trust model considers the impact factors, the more convincing the trust evaluation result.
- Generality (G): the trust model for social networking can be commonly or widely used in different social networking application scenarios.

3. REVIEW

We review existing work about trust evaluation in the social networking in recent years. Certain search criteria are used to gather literature work. We use the keywords: trust evaluation or trust assessment or trust generation or reputation generation or reputation assessment or reputation evaluation or trust management or reputation system, and social networking, to search in all authoritative databases, such as IEEE Explorer, ACM library, Springer library, and Science Direct. We classify our review based on the approaches to build trust model: trust models based on static data, trust models based on dynamic data, hybrid trust models and other models. We treat user profiles, past experiences and interests, etc. as static data; user interaction and user votes, etc. as dynamic data. Hybrid trust models use both static data and dynamic data to compute a trust value. Other models are the models that are not entirely in line with the above classification.

3.1 Static Data Based Trust Models

Since people and their acquaintances are connected with one another to form a social network, it is an effective method to calculate a trust value based on previous experiences and knowledge of acquaintances. Positive experiences and same interests can lead entities in a same community to interact more frequently.

A "mobitrust" model that encompasses three static factors: the similarity of user profile, past experiences and history of friendship was proposed in [4]. The three factors were given different weights(α, β, γ) and influence the trust value in an integrated way. The user profiles were assumed to be composed of a set of keywords. They adapt the private set intersection protocol that based on the use of homomorphic encryption and balanced hashing to protect users' private information. In the protocol, supposing that party A has profile set $\{a_1, a_2, a_3, a_4\}$, party B has profile set $\{b_1, b_2, a_3, a_4\}$, both A and B can only learn that $\{a_3, a_4\}$ is the intersection set. So the model satisfies the item "Pr" since no user can learn more than the computed intersections of their private profiles. The reputation includes A's personal observation of B's reputation and B's global reputation, which are decided by certain percentages. It satisfies the item "Us" since it concerns user profiles. The trust factor based on history of "friends" utilizes the transitive property of trust. The more friends two users share, the more they can trust each other. Above all, this paper proposed a trust model that encompasses three important factors special for spontaneous mobile social networking. It did not consider dynamic data that plays an important role in trust evaluation, thus it does not satisfy the criterion "C". In their experiments, they

analyzed the ability of the trust model to distinguish bad nodes, however, the result was acceptable to some extent. Thus the criterion "T" is partially supported and the criterion "Ac" is somehow satisfied. What's more, this model was fully decentralized and self-managed, an application applying this model can set the value of α, β andγ, according to different situations, so the criterion "Ad" cannot be fully satisfied in an autonomic way.

3.2 Dynamic Data Based Trust Models

User interaction reflects user behaviors in the social networking, which is an important aspect to compute social trust. Many researches on behaviors of users have been widely reported in the fields of psychology, social science, behavior science and system design [12].

Lin et al. proposed a "trust and distrust" mechanism in a recommendation system [2]. In this scheme, they calculated trust score based on previous interaction between a receiving agent and a sending agent. The receiving agent increases the trust score of the sending agent by one unit when it receives a recommendation that is perceived to be correct. The receiving agent decreases the trust score of the sending agent by one unit when it receives a recommendation that is perceived to be incorrect. The same is applied to calculating the distrust score. When the level of distrust score exceeds a certain threshold for an acquaintance, recommendations received from the acquaintance will not be considered during a decision making process until the level of distrust is below the threshold. At the end, the authors utilized software agents connected with one another via social networking to model the behavior of people. The result showed that the average number of recommendations received for each request drop significantly with the distrust score. So we believe this model also satisfies the criterion "Ac".

Guo et al. proposed a fine-grained attribute-based reputation system in [3]. It represents users' reputation in terms of attributes and enables users to rate each other's attributes instead of real identities. First, this model collects people's recommendations. Second, the privacy of users' voting attributes and voters' identities has been protected. In this model, an attribute can be verified without revealing the linkage between the identity and the corresponding attribute. It uses voter anonymity and vote receiver anonymity for preserving identity privacy. Thus it satisfies the criterion "Pr". In this model, to guarantee the authenticity of the reputation value that only relies on contents rather than a content generator, the model leverages zero-knowledge proofs to let voters use verified attribute values to vote instead of arbitrary unauthorized or unauthentic users. So the model unifies user's voting with trustworthy credibility, it satisfies the item "Un". Simulations showed the computation cost contrast between voters and vote receivers in equality check and anonymous voting process. The vote receivers spend less time than the voters. However, system run time analysis with encryption impaction was not investigated to show its efficiency by comparing with similar existing models.

Weitzel et al. provided a new methodology to rank reputation in a network structure based on weighted social interaction [7]. They focused on microblogging services and used a "reweet" mechanism as interaction tool to infer reputation. It is believed that, when A "reweet" B's post, B's reputation will be increased by sharing B's post with A's followers or contacts. To meet the objective of the proposal, they created a network structure based on retweet weighted ties named Retweet-Network and a binary network, named RT-Binary to evaluate the quality of proposed approach. Obviously, this model concerns "Us". However, it can only be used in a certain scenario and does not consider user privacy, so criteria "G" and "Pr" are not satisfied.

Similarly, Adali et al. evaluated trust based on communication behavior of members in a social network [9]. They focused on two particular behaviors as an expression of trust: conversation and propagation. Conversation trust specifies how long and/or how frequently two members communicate with each other. Longer or more frequent communication indicates more trust between the two parties. For the propagation trust, if B propagates information from A often, then they proposed that B must be trusting A. What's more, propagation trust is measured using only statistical communication data without semantic information in order to protect user privacy. However, if B propagates opposite information from A often, it cannot illustrate B trusts A. So the criterion "Ad" is unsatisfied. What's more, performance evaluation is not sufficient. Robustness and efficiency were not proved, similar to [7]. But this model can automatically perform trust evaluation based on user interaction, thus the criterion "Us" is satisfied.

Carchiolo et al. proposed a distributed and secure algorithm based on TrustWebRank, a metric that takes into account both personalized trust evaluation and network dynamics issues [8]. Personalization means that different trust values can be assigned to the same user by different persons, rather than having a single (global) trust value for a given user. In their proposal, both evaluation and storage are distributed, and each node i is responsible for computing and storing its indirect trust T_{ij} for node j. So the criterion "Us" is satisfied. Considering network dynamics means designing a proper mechanism to cope with the (possibly rapid) change of trust values. So the criterion "Ad" is satisfied. In addition, distributed implementation is useful because centralized approaches become more and more unfeasible as the size of networks increases, and they suffer from a single-point-of-failure in terms of both reliability and security. The real effectiveness of such a distributed algorithm depends, however, on its performance in terms of memory usage and execution time, hence, they evaluated both the traffic generated across the network and the time needed to converge to significant values in experimental evaluation. Results showed that the proposed distributed algorithm is effective and efficient, while preserving original benefits of TrustWebRank. So the criterion "E" is satisfied. Since each node computes and stores its indirect trust about other nodes, malicious nodes might report false values of their own vector. Then the authors proposed a secure version aiming at resisting the attacks of malicious nodes. However, it consumes much time and money. So the algorithm satisfies the criterion "T".

Ortega et al. proposed a system intended to propagate both positive and negative opinions of users through a network [14] that is similar to the mechanism in [2]. Their approach is intended to build a ranking of users according to their trustworthiness, demoting the users who present a dishonest behavior in the system. They proposed an algorithm called PolarityRank that extends the PolarityRank algorithm to propagate positive and negative information through a graph. In their scheme, they took the users of the network as the nodes of the graph, the edges represents the opinions of some users about others, and the weights of the edges corresponding to the intensity of the relationship between the nodes. The intensity of the relations can be measured depending on different types of social network that they are processing. This satisfies the criteria "Us" and "G". Some social networking have a special group of users called moderators, whose opinions are more important than the opinions from the rest of the users. In their system, they also considered this circumstance indicating that the model is adaptive to context changes, thus satisfying the criterion "Ad". In addition, the proposal has been evaluated in different challenging situations, such as the generation of random graphs. It is intended to show the performance of their approaches against the basic attacks. They analyzed the error rate of the trust model against five different threat models compared with some existing trust models. The results showed that the model they

proposed performs very well in every situation, showing that the propagation of trust and distrust is a reliable mechanism in a Trust and Reputation System. So this model satisfies the criterion "T". However, the trust model in [2] has not considered the dishonest vote attacks, if there are many dishonest nodes spread bogus opinions, the accuracy will be highly decreased.

3.3 Hybrid Trust Models

Yan et al. motivated protecting Pervasive Social Networking (PSN) by controlling its data access in a heterogeneous manner based on two dimensions of trust levels [5]. The proposed scheme seamlessly incorporates a hybrid trust management framework for PSN by applying Attribute-Based Encryption (ABE). Concretely, the scheme can achieve fine-grained access control and remove the complexity of hierarchical attribute-based fine-grained access control by replacing it with two dimensions of trust levels. They evaluated the trust levels according to many factors and simplified the ABE attribute structure by only considering the trust levels. This scheme satisfies the criterion "C". Since this scheme reduces the complexity of the access policy description and meanwhile keeps its expressivity, it can be flexibly applied into many scenarios by cooperating with a trust management framework. So the criterion "G" is also satisfied. The scheme not only supports controlling PSN data access based on accurate general trust (GT) evaluation by an authorized party but also achieves effective data protection based on the trust evaluated by PSN nodes. So the criterion "Ac" is satisfied. This scheme supports applying node pseudonyms in PSN in order to ensure an expected level of privacy and security, so the criterion "Pr" is satisfied. The PSN can be automatically secured since the related cryptographic keys can be automatically managed based on two dimensions of node trust levels, node revocation, and the validity period of the keys. This fits the criterion "Ad". What's more, the extensive analysis and performance evaluation based on implementation further showed that the proposed scheme is highly efficient. So the criterion "E" is supported.

Yan et al. proposed a scheme to securely control data access by evaluating trust value based on both static data and dynamic data [6]. In the scheme, there are two different kinds of entities; the mobile users who use their mobile devices to interact with a cloud service provider (CSP) and the CSP that can be accessed by all users and other CSPs that store personal and private data of users in the data center. When user A saves his sensitive personal data at the CSP data center, while user B would like to access it with the authorization of A. A will conduct trust evaluation based on mobile social networking activities, behaviors and experiences. This fits the criterion "C". While, CSP's reputation is evaluated according to its user's feedback which is dynamic. If CSP gets bad user's feedback, it will be punished in order to encourage and ensure good behaviors of CSPs. According to the trust level and its linked context, the data owner encrypts his/her personal data by setting the trust threshold and specifying access context for the encrypted data access. The data owner issues the decryption keys to eligible users. Thus, personal data access (with conditions like the trust level being higher than a pre-defined threshold in a specific context) can be fully controlled by the data owner. Due to the dynamic changes of trust levels, the data owner informs CSP the blacklist of the users who are not eligible to access the data according to new trust assessment results. This supports the criterion "Ad". They ensured the CSP to perform the above additional access control following the data owner's expectation based on a reputation mechanism. Each CSP's reputation is evaluated according to its user's feedback and published in order to encourage and ensure good behaviors of CSPs. Trust evaluation can be automatically conducted based on collected data without user involvement, thus the criterion "Us" is supported. In addition, the proposed scheme can be flexibly applied into many scenarios by cooperating with a trust management framework. Since context-awareness is easy to be supported by applying context-aware trust assessment. So the criteria "G" and "Ad" are satisfied. What's more, the comparison with existing work showed its efficiency, satisfying the criterion "E".

Caverlee et al. presented a social trust framework called SocialTrust for enabling trusted social information management in Internet-scale social information systems [10]. Three salient features of the model they proposed are as follows. First, SocialTrust augments the relationships in the social network with a personalized feedback mechanism so that a user's trust value can reflect his behavior (via feedback) as well as the user's position in the social network. Second, SocialTrust distinguishes user relationship quality from the trustworthiness of the user, leading to better resistance to trust manipulation. Third, the model considers the history and the immediate user behavior change, which can mitigate the impact of malicious participants who build up a good trust value over time (through the other two components) and suddenly ''defect." So the criterion "Ad" is supported. At last, they experimentally evaluated the SocialTrust framework using real online social networking data consisting of millions of MySpace profiles and relationships. They tested the robustness of the framework, the results showed that SocialTrust supports robust trust establishment even in the presence of large-scale collusion by malicious participants. So the criterion "T" is satisfied.

In social science, trust is known as a complex term with multiple facets, which has not been well exploited in prior recommender systems. In [15], Fang et al attempted to address this issue by proposing a trust and distrust framework with considerations of both interpersonal and impersonal aspects of trust and distrust. Specifically, four interpersonal aspects (benevolence, competence, integrity and predictability) are computationally modeled based on users' historic ratings, while impersonal aspects are formulated from the perspective of user connections in trust networks. So the criterion "C" is satisfied. Two logistic regression models were developed and trained by accommodating these factors, and then applied to predict continuous values of users' trust and distrust, respectively. After learning the two logistic regression models, (implicit) trust and distrust values are predicted, where the trust values are further refined by the distrust values. These newly generated trust values are taken as input to three representative trust-based recommendation algorithms (i.e. TidalTrust, Merge and SocialMF) in order to validate the effectiveness of the proposed model.

Most of the first generation reputation management system (RMS) are yet very basic, ad hoc and often vulnerable to various attacks. In [13], Khan and Shaikh took a holistic approach to this interesting problem of RMS design. They proposed a generalized set-theoretic phenotype reputation function where its specific components can be customized to meet the reputation requirements of wide variety of reputation assessment needs encountered in today's online activities. This paper proposed a generic reputation function, which can be customized to be used in various reputation scenarios. Thus, it supports the criterion "G". The core factors that can affect the reputation of an individual were identified. In most of the other reputation functions, the core factors are static whereas in the proposed function they can be changed according to the demands of the environment. So the criteria "C" and "Ad" are satisfied. In the reputation system, one of the factors must be the opinions from the users, no matter consider whether who are the users or not. So "Us" is satisfied. The attack tolerance was analyzed against various socio-communal reputation attacks such as gang attacks. Thus, the criterion "T" is concerned.

Jiang et al. proposed a recommendation-aware trust evaluation model in social networking [16]. In their model, they aimed at selecting proper recommendations to predict the trustworthiness of an unknown target. And the criteria to measure and adjust the quality of recommendations include four aspects: the preference of a user, how much a friend knows the source or the target, the historical behavior and fluctuation of one's friends, and the cost and availability of the friend as a recommender. So the criteria "Us" and "C" are concerned. They also proposed algorithms respectively considering two scenarios: multihops are needed to reach a target; multitargets are involved to estimate trustworthiness. The proposed model is efficient to dynamically manage trust relationships, satisfying the criterion "E". The effectiveness of the recommendation-aware trust model was evaluated with experiments with two real social network datasets. However, the model cannot be applied into real trust evaluation applications in a generic way. Thus, the criterion "G" cannot be supported.

Falcone et al. focused on the research topic that if agent X acquires information from a source B, how to measure the relevance and trustworthiness of information [17]. They proposed an interactive cognitive model to evaluate the trustworthiness of source B by combining competence and reliability, which calculated by three aspects: previous direct experience, recommendations (other individuals reporting their direct experiences and evaluation about B) or reputation and the categorization of B. They made the trust evaluation considering three circumstances and did the simulation to show evaluation effectiveness respectively. Thus, the criterion "Ac" is concerned. However, in their case, the additional information on the trustee is free of cost; but in general, accessing this information should take cost into account. What's more, in their research, it is assumed that a source can be categorized and that this category is known. Thus, the criterion "G" is not satisfied because this model's application scenario is limited.

Meo et al. presented a user-to-groups (U2G) algorithm to solve the problem of optimal matching between the individual users' profiles and the profiles of the groups in an Online Social Networking (OSN) scenario [18]. They measured the compactness of the users or groups on the degree of similarity and trust level. The similarity between the profile of user A and user B depends on four factors: interests, access preferences, behaviors and friends. These are static data, however, trust must be evaluated by collecting the users' subjective opinions that are dynamic data. So we classified the algorithm into the hybrid ones. The U2G algorithm is flexible with some modifications that can implement different cost functions to associate users with groups. The applicability of the proposed algorithm was also studied. On one hand, the algorithm can be used in recommender systems to make a prediction of user satisfaction when joining into a given group, based on the computation of the new compactness that the group would assume if a user would like to join into it. On the other hand, the algorithm can also be implemented by a recommender agent associated with a given group, which will act as a counselor for a group administrator. Based on the above, it is obviously that the criteria "Us", "C", "Ad", and "G" are satisfied.

3.4 Other Models

In the current literature, graph theory is widely applied in the field of social network modeling. Researchers tried to use the graph theory to quantitatively analyze social networking and have achieved promising results. Jiang et al. focused on generating small trusted graphs for large OSNs, which can be used to improve two common problems in large OSNs: (1) too complicated to get or maintain information used to construct trust; (2) the information to build trust model is usually subjective and changeable [1]. They proposed a novel user-domain based trusted acquaintance chain discovery algorithm for preprocessing a large social network, based on the theory of ''weak ties''. Then, they presented how to build a trust network and generate a trusted graph with an adjustable width breadth-first search algorithm. In this approach, they considered the users opinions to evaluate the target entity. To validate the effectiveness of their work, they conducted many experiments with the real data set collected from Epinions.com. The experiments for connection coverage showed the efficiency of their trust model and verified the small-world network theory in that the coverage is more than 92.8% when max length is 6, this satisfies the criterion "E". The experiments for accuracy evaluation showed that the generated trusted graphs perform well when predicting trust. Thus, the criterion "Ac" is supported. What' more, they also tested the robustness with respect to different percentages of vicious nodes. From the results, we can see that the accuracy is relatively high: even when 70% of nodes are bad nodes. So the criterion "T" is highly satisfied.

Conte et al. proposed a novel approach to address the issue of evaluating the trustworthiness of the contacts of a social networking user [11]. This approach relies on a multi-layer graph, which models the multiple interactions of a smartphone user with its multiple social media. Such a model, improved by overlap metrics, allows important contacts to be identified and to integrate such contacts into the evaluation of trust. The approach was tested based on the data of a set of social networks (Address Book, Twitter, Google and Facebook) extracted from smartphones and a set of contacts (friends and non-friends) extracted from Facebook and Twitter. The results proved the efficiency of the approach, thus the criterion "E" is satisfied. In this approach, trust evaluation does not require any user participation and it only relies on data available locally on the smartphone. The analysis was performed in the user's smartphone. No rule of confidentiality is violated and no special access to information is required.

3.5 A Summary and Comparison

In Table 1, we give a comparison of the reviewed literature. Y represents that a trust evaluation model supports or satisfies the underlying property. N represents that the property cannot be satisfied or supported. P represents that a trust evaluation model satisfies the property partially. Blank represents the property has not been mentioned or considered in the work.

Table 1. Comparison of reviewed work

Papers	T	Ad	Us	Pr	Ac	E	Un	C	G
[4]	P	N	Y	Y	Y	-	-	N	-
[2]	N	-	-	N	Y	-	N	-	-
[3]	-	-	Y	Y	N	-	Y	-	-
[7]	-	-	Y	N	-	-	-	-	N
[9]	-	-	Y	-	N	N	N	N	N
[8]	Y	Y	Y	N	-	Y	-	-	-
[14]	Y	Y	Y	-	Y	N	-	N	Y
[5]	-	Y	-	Y	N	Y	N	N	Y
[6]	-	Y	Y	N	-	Y	-	-	Y
[10]	Y	Y	-	-	-	N	-	-	-
[15]	-	-	-	-	N	-	N	Y	-
[13]	Y	Y	Y	N	N	-	N	Y	Y
[16]	-	-	P	-	-	Y	-	P	-
[17]		-	Y	-	Y	Y	-	-	-
[18]	-	Y	Y	-	-	-	-	Y	Y
[1]	Y	-	-	-	Y	Y	-	-	-
[11]	Y	-	N	N	N	Y	N	N	-

4. FUTURE RESEARCH TRENDS

According to the above analysis, we suggest a number of promising research directions about trust evaluation in social networking as follows.

A. Enhance the trustworthiness of trust evaluation

The ability to resist malicious attacks is a significant aspect of a trust system. Sherchan et al. also highlighted the importance of trustworthiness in trust models [12]. However, many trust schemes focus more on effectiveness rather than trustworthiness, and we can conclude that only half of the reviewed articles discussed the trustworthiness of trust evaluation to overcome various potential attacks. Most articles did not demonstrate this aspect, or only discussed one possible attack the model may confront. However it is better to consider the various kinds of attacks the proposed model can resist, especially with efficiency evaluation performed.

B. Preserve user privacy with efficiency

Since the main purpose of social networking is to provide a forum for free and unhindered communications, privacy concerns create a major roadblock in achieving this goal. Any social networks would therefore need to address the privacy issue in order to be unconditionally accepted by their users and ultimately achieve final success. Many trust models [4, 16, 17, 18] measured the trust value based on the users past experiences or profiles. This could cause privacy leakages. Meanwhile, some models tried to solve this problem by using encryption [3, 4, 6]. However, computation cost is obviously increased due to key management. How to preserve the privacy in a light way could be an interesting future research direction.

C. Improve applicability and generality

There are many kinds of social networks. If a trust model can be evaluated or proved as effective in most application scenarios, it should be especially valuable. However, the application scenarios have rarely been discussed in the reviewed literature and most existing trust models only focused on improving the quality and performance in some certain aspects. Even though a trust model cannot be used in some scenarios, the authors should have a discussion on why the model fails to fit that application scenario. This may motivate other researchers to improve the model.

D. Combine trust and distrust in trust modeling

A distrust value is as important as a trust value, such as in on-line marketplaces where the potential buyers not only evaluate the price of a product but also the reputation of a seller. In this case, negative feedback from a customer can strongly influence the decisions of other users about that seller. The negative opinions are also important in social networks for review aggregation, social news propagation and recommender systems. Some work [2, 14, 15] proposed merging distrust in trust modeling. The good impact of distrust value was illustrated in trust modeling. So, in our opinion, it is beneficial to combine trust and distrust in the trust model.

E. Enhance adaptability for big data network

Social networking is a social structure made up of a set of social actors, sets of dyadic ties, and other social interactions that can carry big data. Many models have been proposed for constructing and calculating trust in normal scale social networking. For example, the trust model in [4] was only evaluated based on the experiments with 2000 nodes. However, in the big data era, it is necessary to develop a trust model suitable for large social networking and supporting big data process. With many new technologies such as data mining merged, it is novel and attractive to use new technologies in trust evaluation in social networking.

5. CONCLUSIONS

In this paper, we reviewed recent work about the trust evaluation in social networking with uniform review criteria. We then proposed some open issues and future research directions in this research field. We found that few trust models have considered the robustness and generality. None of them satisfy all criteria holistically. Moreover, the reviewed work showed that it is hard to preserve user privacy with low computation complexity, which should be a promising future research topic. We also proposed that since social networking contains massive data, applying some emerging technology like data mining in trust evaluation could be a novel research topic.

6. ACKNOWLEDGMENTS

This work is sponsored by the NSFC (grant U1536202), the 111 project (grant B08038), the PhD grant of the Chinese Educational Ministry (grant JY0300130104), the Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2016ZDJC-06), and Aalto University.

7. REFERENCES

[1] Jiang, W. J., Wang, G. J., and Wu, J. 2014. Generating trusted graphs for trust evaluation in online social networks. *J. Future. Gener. Comp. Sy.* 31, (Feb. 2014), 48-58. DOI = http:// dx.doi.org/10.1016/j.future.2012.06.010.

[2] Lin, C. C., Lin, T. S., and Liu, W. Y. 2012. A trust and distrust mechanism for a social network-based recommendation system. In *15th International Symposium on Wireless Personal Multimedia Communications* (Taipei, Taiwan, September 24-27, 2012). WPMC'12. IEEE, Washington, DC, 172-176.

[3] Guo, L., Fang, Y. G., and Wei, L. B. 2013. Fine-grained privacy-preserving reputation system for online social networks. In *IEEE/CIC International Conference on Communications in China* (Xi'an, China, August 12-14, 2013). ICCC'13. IEEE, Washington, DC, 230-235. DOI = http:// dx.doi.org/10.1109/ICCChina.2013.6671120.

[4] Li, J., Zhang, Z. H., and Zhang, W. Y. MobiTrust: trust management system in mobile social computing. In *Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology* (Bradford, UK, June 29-July 1, 2010). CIT'10. IEEE, Washington, DC, 954-959. DOI = http:// dx.doi.org/ 10.1109/CIT.2010.176.

[5] Yan, Z., and Wang, M. J., Protect Pervasive Social Networking Based on Two-Dimensional Trust Levels. *J. IEEE. Syst. J.* 441, 6 (Sep. 2014), 1-12. DOI = http:// dx.doi.org/: 10.1109/JSYST.2014.2347259.

[6] Yan, Z., Li, X. Y., and Kantola, R. 2014. Personal data access based on trust assessment in mobile social networking. In *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* (Beijing, China, September 24-26, 2014). TrustCom'13. IEEE, Washington, DC. 989-994. DOI = http:// dx.doi.org/ 10.1109/TrustCom.2014.131.

[7] Weitzel, L., de Oliveira, J. P. M., and Quaresma, P. Exploring trust to rank reputation in microblogging. *Proceedings of the 24th International DEXA Conference* (Prague, Czech Republic, August 26-29, 2013) DEXA'13. Springer-Verlag, Berlin, Heidelberg, 434-441. DOI = http:// dx.doi.org/ 10.1007/978-3-642-40173-2_36.

[8] Carchiolo, V., Longheu, A., Malgeri, M., and Mangioni, G. Trust assessment, a personalized, distributed, and secure approach, *J. Concurrency and Computation, Practice and Experience*, vol. 24, no.6, pp.605-617, 25 April 2012

DOI = http:// dx.doi.org/10.1002/cpe.1856.

[9] Adali, S., Escriva, R., and Goldberg, M. K. et al. Measuring behavioral trust in social networks. In *IEEE International Conference on Intelligence and Security Informatics* (Vancouver, Canada, May 23-26, 2010). ISI'10. IEEE, Washington, DC. 150-152. DOI = http: // dx.doi.org/ 10.1109/ISI.2010.5484757.

[10] Caverlee, J., Liu, L., and Webb, S. 2010. The social trust framework for trusted social information management, architecture and algorithms. *J. Inf. Sci.* 180 (Jan. 2010), 95-112. DOI = http:// dx.doi.org/ 10.1016/j.ins.2009.06.027.

[11] Perez, C., Birregah, B., and Lemercier, M. 2013. A smartphone-based online social network trust evaluation system. *J. Soc. Netw. Anal. Min. 3* (Dec. 2013), 1293-1310. DOI = http:// dx.doi.org/ 10.1007/s13278-013-0138-4.

[12] Sherchan, W., Nepal, S., and Paris, C. 2013. A survey of trust in social networks. *J. ACM Comput. Surv.*45, 4 (Aug. 2013), 115-123. DOI = http: //doi.acm.org/10.1145/2501654.2501661.

[13] Khan, J. I. and Shaikh, S. S. 2009. A phenotype reputation estimation function and its study of resilience to social network. *J. Netw. Comput. Appl*. 32, 5 (Jul. 2009), 913-924. DOI = http: // dx.doi.org/10.1016/j.jnca.2008.12.003.

[14] Ortega, F. J., Troyano, J. A., Cruz, F. L., Vallejo, C. G., and Enriquez, F. 2012. Propagation of trust and distrust for the detection of trolls in a social network. *J. Computer Netw*. 56 (Aug.2012), 2884-2895. DOI = http: // dx.doi.org/10.1016/j.comnet.2012.05.002.

[15] Fang, H., Guo, G. B., and Zhang, J. 2015. Multi-faceted trust and distrust prediction for recommender systems. *J. Decis. Support. Syst.*71 (Feb.2015), 37-47. DOI = http:// dx.doi.org/10.1016/j.dss.2015.01.005.

[16] Jiang, W. J., Wu, J., and Wang, G., J. 2015. On selecting recommenders for trust evaluation in online social networks. *ACM Trans. Internet. Techn.* 15, 4 (Dec. 2015), 1-21. DOI = http://doi.acm.org/10.1145/2807697.

[17] Falcone, R., Sapienza, A., and Castelfranchi, C. 2015. The relevance of categories for trusting information sources. *ACM Trans. Internet. Techn.* 15, 4 (Dec. 2015), 852-861. DOI = http://doi.acm.org/ 10.1145/2803175.

[18] Meo, P. D., Ferrara, E., Rosaci, D., and Sarne, G. M. L. 2015. Trust and compactness in social network groups. *J. IEEE T. Cybern.*45, 2 (Feb. 2015), 205-216. DOI = http: // dx.doi.org/ 10.1109/TCYB.2014.2323892

[19] Yan, Z., and Holtmanns, S. 2008. Trust modeling and management: from social trust to digital trust. In R. Subramanian (Ed.) Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions. IGI Global. 279-306. DOI= http:// dx.doi.org /10.4018/978-1-4666-2803-8.ch018.