Artif Intell Rev
DOI 10.1007/s10462-017-9583-1

TP-TA: a comparative analytical framework for trust prediction models in online social networks based on trust aspects

Aynaz Khaksari[1] · MohammadReza Keyvanpour[1]

© Springer Science+Business Media B.V. 2017

Abstract Formation of online social network (OSN) strongly depends on the quality of relationships between its agents. Such relationships are affected by a host of factors; trust is one of them. To enhance the quality of relationships in such networks, it is important to find a mechanism to predict the degree of trust among participating agents since trust is the major driving force for initiating and developing social relationships. Although much effort has been made to develop quantitative techniques to obtain trust value, there is a lack of coherent classification of such techniques to achieve a macro vision of trust prediction models and identify their strengths and weaknesses. In this paper, we proposed TP-TA, an analytical framework which consists of three main components: First, classification of various existing trust prediction models in terms of trust aspects in the context of OSNs. Besides, main ideas, prospects, and challenges of each approach are highlighted for further research in this field. Second, defining general criteria to analyze our proposed classification. Finally, we illustrate a qualitative comparison between each approach which is a guide to understanding their superiority to one another. This framework could lead to an efficient selection of trust prediction techniques based on the nature of the target OSN and the intended trust type.

Keywords Online social networks · Trust prediction · Approaches · Challenges · Benefits · Trust prediction model selection · Analytical comparison

1 Introduction

As OSNs have become more increasingly integrated with our life, issues related to their proper use have become more important. Highly dynamic status of OSNs with continuously joining and leaving agents and also its web-based nature create an open and unsecured

✉ Aynaz Khaksari
akhaxari@gmail.com

[1] Engineering Department, Alzahra University, Tehran, Iran

Published online: 22 October 2017

environment. People are in interaction without knowing each other and disclose their information. According to a phenomenon called Privacy Dilemma (Brandtzaeg et al. 2010), "although users are aware of risks of sharing information in OSNs, their online activities do not reflect their concerns". Providing security and high-quality relationships in such open networks is a complicated scenario. The most challenging part of this scenario is that we should ensure that potential partners will not harm each other (Liu et al. 2015). In this case, trust can be a solution. Determining the validity of each agent, detecting untrusted agents, checking the relationship between agents to understand their latent behavioral patterns and to predict the quality of their future relationship, allowing trustworthy agents to have an impact on others and etc are just part of necessary actions to make OSNs environment trustful. In fact, OSNs form in the context of trust because trust plays an important role in initiating and developing relationships, improving their quality level and making them more stable. Estimating the degree of trust among potential partners can also be helpful in decision making; people tend to be more open to advice from their trusted referrals. In this regard, recommender systems which benefit from trust have attracted significant attention (Massa and Avesani 2006; Fang et al. 2014; Shuiguang et al. 2016).

Trust relationships are hard to model for computer scientists and quantifying trust in OSNs is a difficult problem, because of the complexity of OSNs and the ambiguity of the concept of trust. Attitudes towards trust are often very different and the highly dynamic nature of OSNs make it hard to implement a robust and efficient mechanism for estimating trustworthiness of agents. To overcome such issues, scientists tend to treat trust in a quantitative manner. To understand the latent intention of potential partners, predicting the degree of trust quantitatively is vital. In the literature, a plethora of trust prediction techniques aimed to assign trust a quantitative value have been proposed; but there are few studies to provide a comprehensive classification of these models which covers all existing works and propose a comparative evaluation.

In this paper, we introduce TP-TA, a comparative analytical framework which consists of three main components, in order to classify existing trust prediction models with respect to different aspects of trust. Besides, by analyzing the extent to which evaluation criteria are met, prospects and challenges are highlighted for further research in this field. The main goal of this paper is to organize, analyze and present trust prediction models in a unified and comparative manner with regard to the problem of predicting and evaluating trust in OSNs. We believe that the three aforementioned goals on which the paper has focused can be helpful both for researchers in this field and for practitioners interested in this topic. For the latter case, our ultimate goal is that this paper can be used as a practitioners guide.

The rest of this paper is organized as follows: At first, we define the concept of trust in Sect. 2 and clarify its different properties, aspects and types. In Sect. 3, we briefly review some existing surveys which proposed a classification of trust prediction models. In Sect. 4, we summarize trust prediction process in OSNs. Next, in Sect. 5, we introduce our proposed framework, TP-TA, by closely studying the approaches used by different trust prediction models in terms of trust aspects and discussing their individual prospects and challenges. Next, we define comparative criteria to present an analytical comparison. Finally, we propose an analytical study of trust prediction models. Finally, in Sect. 6, we discuss implications and benefits of our proposed framework to determine the applications of TP-TA and possibly future works and directions.

2 Trust: definition and aspects

2.1 Definition and properties of trust

Before explaining trust prediction in OSNs, we should answer a vital question: "what is trust?" Determining this topic can help us to reach an efficient trust prediction mechanism to predict trust value closer to the reality.

Trust is an important topic of research in many fields including sociology, psychology, economics, business and computer science. In the field of computer science, trust is popular as a heterogeneous concept and consists of multiple aspects (Fang et al. 2014). In fact, trust has a multidimensional and ambiguous nature and thus proposing a formal definition of this term is deeply related to the target field (Bhuiyan et al. 2010). With considering such ambiguity, we collect some proposed definitions of trust in the field of computer science that could lead us to extract basic properties of trust.

Sztompka presents a general definition of trust in Sztompka (1999): "Trust is a bet about the future contingent actions of others". This definition consists of three parts: (1) belief, (2) commitment, (3) uncertainty. First, the trustor believes that his/her partner will act in the desired way and perform an expected action. The belief is not the only argument for the existence of a trust relationship. Trust occurs when there is a minimum level of trustee's commitment to accomplish a particular action in the way that satisfies the trustor. This belief is usually formed by personal feelings and intellectual backgrounds. This means trust is a subjective concept and is affected by the trustor's taste (Yan and Holtmanns 2007; Bhuiyan et al. 2010; Yan et al. 2013; Jiang et al. 2016). Subjectivity is defined as the trustor's belief about the level of trustees commitment about a particular action (it's not about the real level of trustee's commitment, it's about the trustor's belief about trustee's commitment). The third part states that trust is a bet and it means there is some kind of doubt and uncertainty in the nature of trust. We can measure the uncertainty of this belief (Adali 2013). The conclusion from this part is that trust is measurable (Marsh 1994). This property of trust can lead us to propose computational models for trust in OSNs. Marsh in his Ph.D. thesis (Marsh 1994) defines trust function between two agents i and j as shown in Eq. (1):

$$Trust(i, j, \alpha) = t, 0 \leq t \leq 1 \tag{1}$$

where α is the situation in which trust occurs. Castelfranchi (2009) provide a more general trust formulation, called the core trust. Core trust is about expectations and evaluations and is defined as follows: Agent i trusts agent j to ensure the goal ϕ by accomplishing the action α if and only if:

1- i wants to achieve the goal ϕ
2- i expects that:

    2-1- agent j has the occasion to ensure ϕ by accomplishing action α
    2-2- j is wishing to accomplish action α
    2-3- the internal preconditions for the execution of action α by agent j hold
    2-4- the external preconditions for the execution of action α by agent j hold

The first item concerns the necessity of achieving the goal ϕ and the latter item concerns the trustor 's attribution of trustee's properties. In this regard, the 2-2 and 2-3 concern what the trustor thinks about the trustee's qualities and dispositions, and 2-1 and 2-4 concern what the trustor thinks about the environmental conditions in which the trustee is going to accomplish

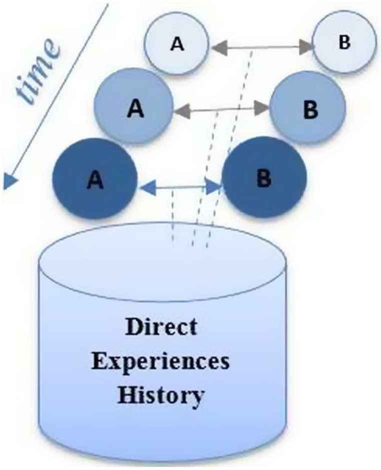


Fig. 1 Reducing the impact of past experiences over time

for achieving the goal ϕ. According to this definition, Castelfranchi (2009) present Eq. (2) which consists of four arguments: trustor, trustee, goal, action.

$$CoreTrust(i, j, \phi) \doteq \vee CoreTrust(i, j, \alpha, \phi)_{(\alpha \in A)} \tag{2}$$

Here, agent i trusts agent j to achieve goal ϕ by action α if and only if there exists some action α in A; where A is the set of actions through which agent j can act toward agent i to ensure ϕ (Cho et al. 2015).

One of the major problems with measuring trust is that it has different meanings in different contexts. In fact, the trustor trusts the trustee to accomplish a specific goal in a specific context (Yan and Holtmanns 2007; Adali 2013). Thus, trust is context specific (Rousseau et al. 1998). Alunkal (2003) define trust as: "the value we attribute to a specific entity, including an agent, a service, or a person, based on the trust exhibited by the entity in the past". We can conclude that the past behaviors of the agent have a great impact on trust value. In fact, trust value increases or decreases with new experiences (Ma et al. 2011). As we show in Fig. 1, new experiences are usually considered more important than old ones. For this reason, trust may change over time as this concept has a dynamic nature and is time-dependent (Sherchan et al. 2013). Also, important experiences have a higher impact than insignificant ones; thus, trust is event-sensitive (Nepal et al. 2010).

In addition, trust is directed (Bhuiyan et al. 2010) and asymmetric (Sherchan et al. 2013); when two individuals are involved in a relationship, trust is not necessarily identical in both directions. This is connected to the subjective nature of trust. Despite of this, members usually act positively with other members whom they trust; thus, trust is self-reinforcement (Sherchan et al. 2013).

Some researchers attribute to trust some degree of transitivity during a chain of agents calling it propagation trust (Gray et al. 2003; Guha et al. 2004; Josang and Pope 2005; Golbeck and Hendler 2006). Trust is not perfectly transitive in the mathematical sense. In some scenarios, because of the propagative nature of information "trust may propagate with appropriate discounting through the relationship network" (Guha et al. 2004) (Fig. 2).

Definition 1 Given two people, A and B, according to trust properties we define trust as follows: *The degree of A's belief (based on his intellectual background and attitudes, B's previous behaviors, A's direct experiences with B or similar users, other people's recommen-*

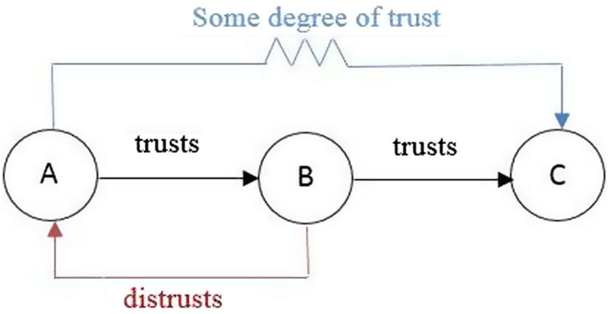


Fig. 2 An example of trust transitivity and asymmetric trust

Table 1 Trust properties

	Trust property	Example
1	Multidimensional	Trust has roots in different disciplines
2	Measurable	*A* may trust *B* more than *C* in the same context
3	Subjective	*A* and *B* propose different definitions of trust based on their own backgrounds
4	Context-specific	*A* may trust *B* in a particular context but distrusts *B* in another context
5	Event-sensitive	The occurrence of an important event can impact the trust between *A* and *B*
6	Dynamic	During the time, the value of the trust between *A* and *B* can be changed
7	Asymmetric	*A* may trust *B*, but *B* may distrust *A*
8	Self-Reinforcement	If *A* trusts *B* then there is high probability that *B* acts positively toward *A*
9	Propagative	If *A* trusts *B* and *B* trusts *C* then there is a high probability that *A* will trust *C*

dations) in the level of B's commitment about future actions in a specific context that lead to an expected outcome that satisfies A.

We summarize the above mentioned trust properties in Table 1.

2.2 Different aspects of trust

Trusting a person is affected by a host of factors, such as: (1) the trustor's predisposition to trust, which is linked to his/her psychology and various events over lifetime; these events can be completely unrelated to the person we are deciding to trust or not to trust; this factor refers to the emotive aspect of trust, (2) other people's opinion of actions and decisions the trustee has had in the past, including his/her reputation and gossip about him/her; this factor refers to the cognitive aspect of trust (Sabater and Sierra 2005; Beatty et al. 2011) and (3) the trustor's relationship and past experiences with the trustee or similar person; this factor reflects the behavioral aspect of trust (Adali et al. 2010). According to these factors, we categorized different types of trust in three major aspects: Emotive, cognitive and behavioral.

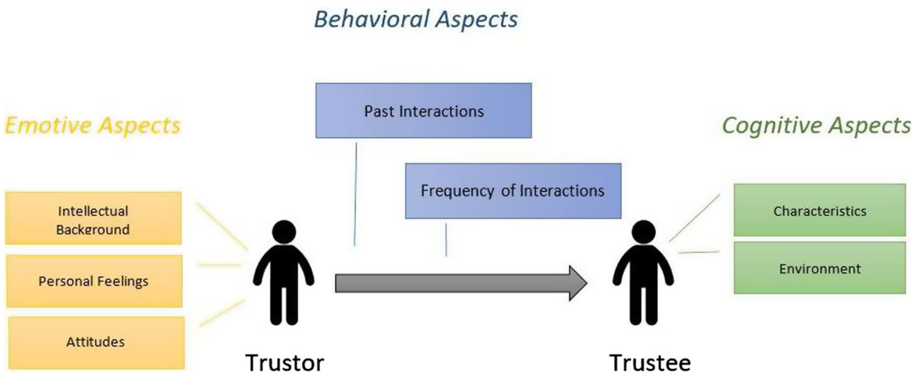


Fig. 3 Boundaries of different aspects of trust

As Fig. 3 shows, this categorization can be concluded from Definition 1. According to Definition 1, the emotive aspect of trust relates to A's belief about B's commitment in an action. Such belief originates from A's feelings about B's previous behaviors, their direct experiences or A's direct experiences with other users who are similar to B. In fact, A observes the situation and makes a decision to trust B or not. Such decision making is affected by A's attitudes, personal feelings and intellectual background which can lead A to make a decision to ignore all the facts about the trustee or lead A to make a decision which is close to the characteristics of the trustee or their relationships. We categorized, trust types which focus on the trustor's properties in Emotive class. In the context of OSNs, because there is no data about such properties, the trustor should explicitly mention his emotions (e.g., rate the trustee after a direct interaction, creating a Web of Trust). In this case, we deal with two different types of trust:

- Identification-based trust: This type of trust means that one person knows another one's personality characteristic. According to Grabner-Kruter and Bitter (2013), it is "the highest and solid level of trust that may be reached by the parties to the trust relationship". In the context of OSNs, it refers to the situation that the trustor knows the trustee in the real world.
- Dispositional trust: Sherchan et al. (2013) describe this type of trust as follows: "general expectations that people develop about trustworthiness of other people over the course of their lives". When the type of relationships and parties are unknown, dispositional trust has a major impact on trusting (Grabner-Kruter and Bitter 2013). In fact, dispositional trust is a psychological trait to be trusting. In the OSN context, it refers to the situation that the trustor doesn't know the trustee and the formation of trust closely related to the trustor's psychological background.

The cognitive aspect relates to B's commitment which totally originates from B's qualitative characteristics, such as competence, ability, integrity, honesty, popularity. This type of trust is connected to a rational calculation of cost and benefits of trusting. In the context of OSNs, such qualitative characteristics can be obtained from B's previous behaviors or can be recommended by other people (e.g., a user has received a lot of endorsements about his proficiencies by reputed experts on LinkedIn, a top trending user on Twitter). In this regard, we deal with:

- Global trust or Reputation: Reputation is what is generally other people said or believed about a person's character (Josang et al. 2007). In fact, reputation is defined by the trust

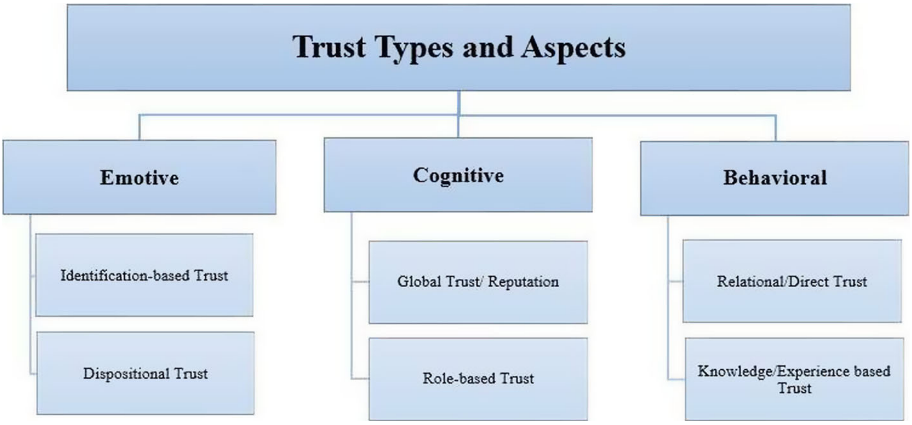


Fig. 4 Different aspects and types of trust

value of all the agents in OSN about a special agent. Most researchers of computational trust have paid a significant attention to this type of trust and in the literature, there is a huge effort to calculate reputation.

- Role-based trust: It refers to the trust coming from considering the trustee's role in OSN. Typically, there are predefined roles in OSNs that help agents to put more trust in one special agent as compared to others (Minhas et al. 2010; Huang et al. 2014). In fact, agents trust each other based on the predefined roles and relationships that exist among them.

The behavioral aspect of trust is based on the observed communication behavior between A/similar users to A and B/similar users to B. The forms of communication used and their frequency between individuals in a social network are in this sense a good indicator of their social relationships and trust (e.g., the fact of having posted something directly on a user's wall on Facebook instead of just having commented on a post left by someone else, the number of times a Twitter user has retweeted a specific user's tweets). In this case, we deal with:

- Relational/Direct trust: It defines trust built up over time as a result of repeated interactions between the trustor and the trustee (Sherchan et al. 2013). Information available to the trustor from within the relationship itself forms the basis of relational trust (Rousseau et al. 1998).
- Knowledge/Experience based trust: It represents a component of trust that is based on direct and repeating interactions among entities during the time (Grabner-Kruter and Bitter 2013). The difference between this type of trust and dispositional trust is that experience-based trust only relies on the results of past direct experiences between two individuals, but in dispositional trust, the trustor considers his past similar experiences.

Figure 4 depicts aspects and types of trust.

3 Related works

In the literature, a plethora of trust prediction models have been proposed. We categorize the existing articles in two broad categories: systems and users. The first category consists of security mechanisms involving policies and security systems in OSNs. The second category is based on trust values gathered and shared by users in OSNs. The main concern of this article is the second category which deals with predicting trust between users and determining the level of reputation. In this section, we briefly review some existing classifications of trust prediction models in this category.

Sabater and Sierra (2005) categorized trust computational models in different dimensions. According to the conceptual model of reference, they classified trust models into two major categories: Cognitive and Game-theoretical. The Cognitive approach refers to user's mental states which causes the user to trust another one. The Game-theoretical approach refers to the result of a more pragmatic game with utility functions, and numerical aggregation of past interactions.

Josang et al. (2007) proposed a classification of trust and reputation computation models with six major classes: Simple Summation or Average of Ratings, Bayesian Systems, Discrete Trust Models, Belief Models, Fuzzy Models. The first category refers to some very basic mathematical function which apply to trust ratings. In the Bayesian Systems reputation, trust value can be represented in the form of the probability expectation value of the beta PDF. Discrete models use discrete values for trust such as Very Trustworthy, Trustworthy, Untrustworthy and Very Untrustworthy, or just simple numerical discrete values. Belief models represent the uncertainty of trust and Fuzzy models represent trust as linguistically fuzzy concepts, where membership functions describe the degree to which an agent can be described as trustworthy.

Victor et al. (2011) classified trust models into probabilistic and gradual categories. A probabilistic approach deals with a single trust value and an agent or source can either be trusted or not and computes the probability that the agent can be trusted. On the other hand, a gradual approach is concerned with the estimation of trust values when the outcome of an action can be positive to some extent, e.g. when the provided information can be right or wrong to some degree, as opposed to being either right or wrong.

Sherchan et al. (2013) classified trust models into three main categories: Graph-based, Interaction-based and Hybrid. The Graph-based approach takes advantages of graph properties such as in-degree, out-degree, density, path, loops and so on. The Interaction-based approach uses interactions and behavioral patterns within the network to compute social trust.

Zheng (2015) categorized trust prediction models into two major categories: static and dynamic. Static category itself consists of two sub-categories: propagation-based approaches and latent factor-based approaches. In the static approach, trust is considered as a fixed value. Propagation-based approaches evaluate trust from a source user to a target user along a path between them consisting of links and trust values. In latent factor-based approaches, trust value can be predicted from the behavior of giving ratings in the trust matrix using latent factor models, such as matrix factorization.

Jiang et al. (2016) proposed a categorization which consists of: D-S evidence theory and subjective logic based approaches, Approaches using traditional mathematics tools, AI and information theory based approaches, Graph-based approaches. The first category focuses on subjectivity of trust by considering uncertainty into account. The second category aims to find a mathematical method for trust computations (e.g. Probability). The third category models trust by learning the problem or decision support system. The fourth category uses graph properties such as those mentioned in Sherchan et al. (2013).

All of these works are one level classifications which evaluate and compare different models with each other. In this paper, we propose a two level classification; we first try to classify trust models into technical categories which are mostly concerned with the algorithmic approach. Secondly, we place them into conceptual categories (trust aspects) which

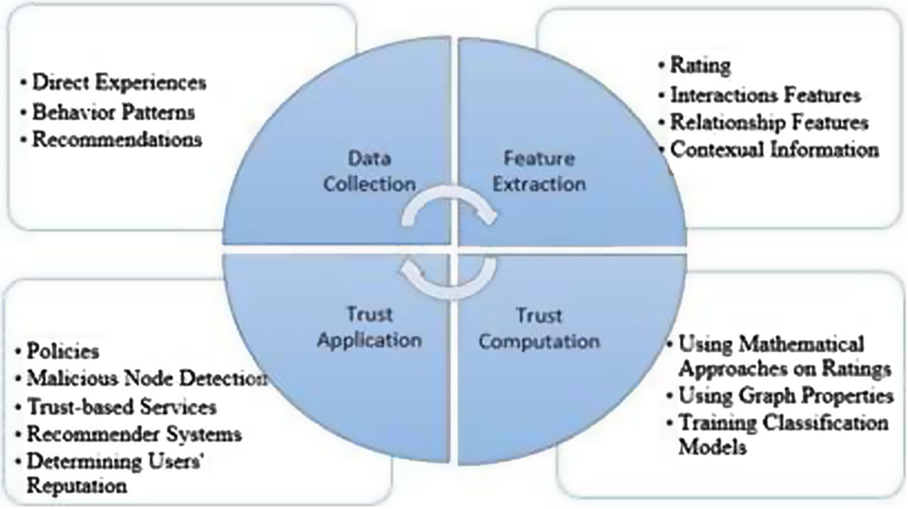


Fig. 5 The process of trust prediction

are strongly related to trust types and properties. Finally, we evaluate and compare our two level categories. We believe this kind of classification could help achieve a macro vision of technical approaches with respect to the concept of trust and also could be more applicable in practice.

4 Trust prediction in online social networks

The main concern about trust in OSNs is predicting its value by analyzing user's information (Yan and Holtmanns 2007). Trust prediction is a technical approach to represent trustworthy level of a potential relationship by a continuous/discrete real numbers or classes. Trust prediction is concerned with the following: collecting the information required to make a trust relationship decision; extracting related features; evaluating the factors which affect on trust relationship and computing new trust value; and applying the predicted value in the target OSN (see Fig. 5).

To collect initial data required for trust prediction, we should specify the source of it. We summarized the most widely used trust information sources in Fig. 6. These sources are divided into first-hand and second-hand in Josang et al. (2007), which first-hand sources carry more weight than second-hand sources. In Josang et al. (2007), the term private information is used to describe first-hand information resulting from explicit feedbacks and behavioral patterns, and public information is used to describe publicly available second-hand information, i.e. information that can be obtained from third parties. Ratings are often used as explicit feedbacks. For example, some agents have an interaction and after that they explicitly express their experience by rating each other. The interaction can be the same, similar or different from past interactions (Tavakolifard 2012; Liu et al. 2015).

Using behavioral patterns of agents is a more efficient method because it is based on implicit feedbacks which means members are not aware of it, but they are able to collaborate calculating trust in an implicit way (Shuiguang et al. 2016). The superiority of behavioral patterns is that it can automatically detect misbehaviors and malicious users. Behaviors of a special agent could be obtained from his past interactions with other agents or the quality

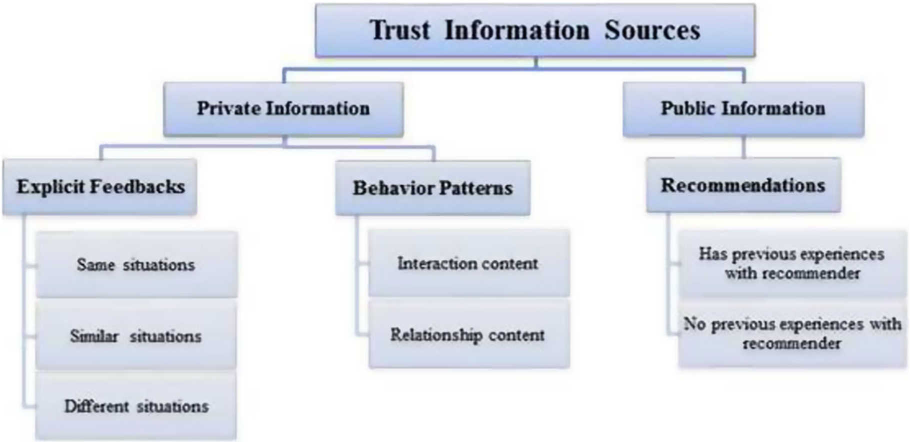


Fig. 6 Classification of trust information sources

of his relationships. In this regard, using contextual information of partners such as role impact factor, reliability preference, social intimacy and etc. could be a way to optimized trust prediction (Zheng 2015).

In the absence of explicit feedbacks and behavior patterns, trust can be based on public information such as recommendations from others. In this case, source agent could have a previous experience with the recommender or not. In the latter situation, contextual information of the recommender such as reputation could lead to a more reliable prediction.

In order to predict trust value from collected data and extracted features, trust should be assigned on a quantitative scale, so we can make computations with trust values in the network (Katz and Golbeck 2006). Trust structure can be presented as a trust network (Fig. 7b) that is a weighted and directed sub-graph $T(V, E)$ for social graph (Fig. 7a) or interaction graph in which trust value between agents is represented as a label for edges and can be shown in an adjacency matrix. A weighted edge that belongs to E from vertex A to vertex B corresponds trust relationship. The weight can be represented by Eq. (3):

$$w(A, B) = V \times V \rightarrow T \tag{3}$$

where T is the trust space and in most cases is in the range of [0, 1] or discrete values and $w(A, B)$ is the level of trustworthy between the trustor A and the trustee B. The main concern of this article is this step and which is studied more closely in the next section. Trust adjacency matrix (Fig. 7c) of a Trust Network can be defined by Eq. (3) for the nodes which are connected by edge, and 0 for the nodes which are not connected.

If the information used for prediction has not been generated in the same context as the trust calculation, then trust adjacency matrix will be a multi-dimensional (Zheng et al. 2014; Shuiguang et al. 2016) as we show in Fig. 8. In this case, considering contextual information is necessary to predict trust value.

After predicting trust value, it should be converted to a usable form to be applied in OSN. In recent years research on trust applications has gained considerable attention and researches have proposed some trust applications in OSNs such as trust based recommender systems (Shuiguang et al. 2016), clustering opinions in OSNs using trust (Xia et al. 2015), malicious user detection, community detection (Pourkazemi and Keyvanpour 2010) etc. But still, there is a huge possibility for research in this area.

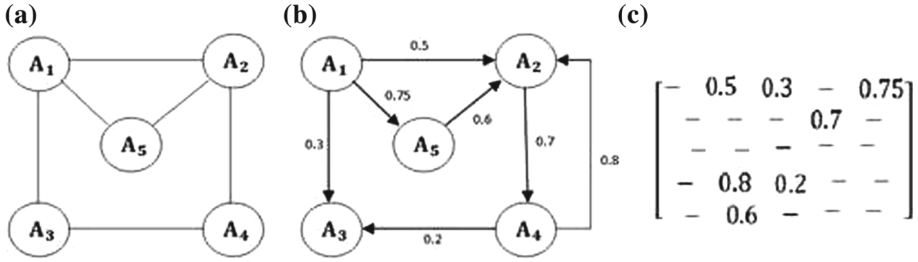
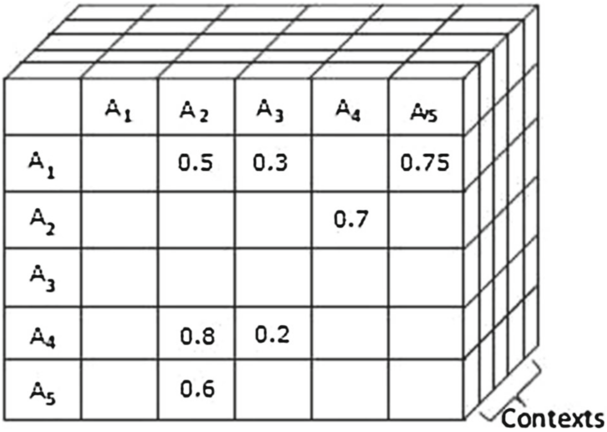


Fig. 7 Trust structure in a single context. **a** Social graph, **b** trust network, **c** trust adjacency matrix



	A1	A2	A3	A4	A5
A1		0.5	0.3		0.75
A2				0.7	
A3					
A4		0.8	0.2		
A5		0.6			

Fig. 8 Multi-context trust adjacency matrix (Zheng 2015)

5 The proposed comparative analytical framework for trust prediction in OSNs

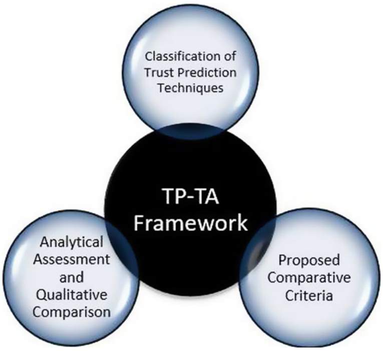
In this section, we introduce TP-TA (**T**rust **P**rediction Models-**T**rust **A**spects) framework. The main idea of TP-TA is the extent of satisfying trust aspects by trust prediction models and highlighting their strengths and weaknesses by presenting an analytical comparison based on assessment criteria. Since we consider different trust aspects and subsequently different trust types which are introduced in Sect. 2.2, our framework could lead to an efficient selection of trust prediction techniques due to the nature of target OSN based on its relevant trust type. As we have shown in Fig. 9, TP-TA consists of three main components:

- Proposed classification of trust prediction models
- Proposed comparative criteria
- Analytical assessment and qualitative comparison

5.1 Classification of trust prediction models

In the literature, a plethora of trust prediction models have been proposed; but there has been little effort to present a comprehensive classification of these models which covers all existing works. As a first attempt, we present a broad categorization of the models that have been proposed so far. This component of TP-TA framework is mostly concerned with

Fig. 9 Main components of TP-TA framework


Classification of Trust Prediction Techniques
TP-TA Framework
Analytical Assessment and Qualitative Comparison
Proposed Comparative Criteria

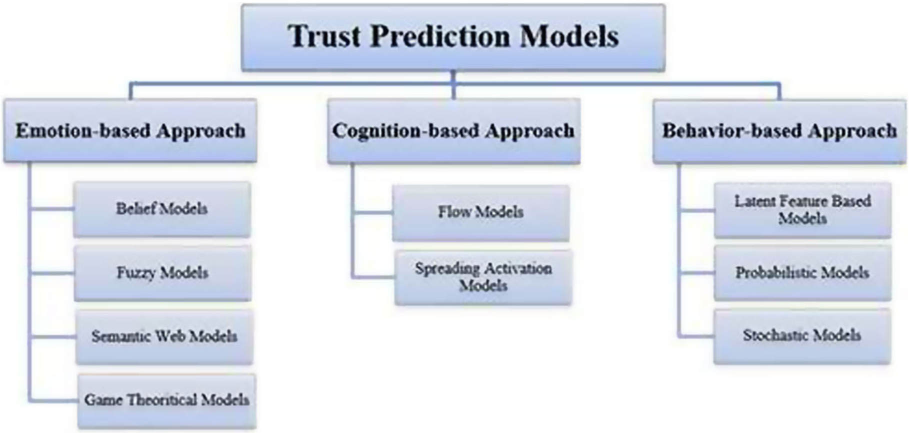


Fig. 10 The proposed classification of trust prediction models based on trust aspects

the methodological principles and the algorithmic approaches. Our proposed classification is based on three aspects of trust that were discussed in Sect. 2.2: emotion-based approach, cognition-based approach and behavior-based approach. Besides, by presenting the prospects and challenges of each approach, there will be an untapped research area for researchers in this field.

Figure 10 depicts schematically our proposed taxonomy of the different approaches for the problem.

In the following, we elaborate on each of these categories in more details, presenting their main ideas, benefits and challenges.

Emotion-based Approach This approach focuses on the emotive aspect of trust and aims to propose efficient usable models for implementing them in real-world OSNs using user's personal feelings. The basic idea of such models is to let agents get involved in assessing each other (Alunkal 2003). As we have shown in Fig. 11, the main source of user personal feelings is his attitudes and intention and also his intellectual backgrounds. Such feelings refer to explicit feedbacks which were discussed in Sect. 4. Subjectivity and uncertainty are the major factors of the user's personal feelings. By specifically considering these two factors,

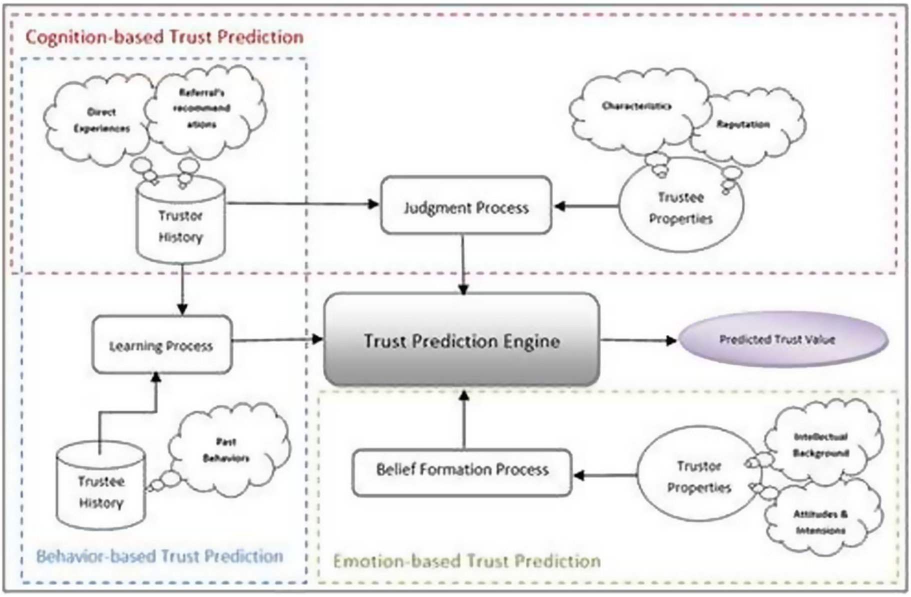


Fig. 11 Different trust prediction processes in terms of trust aspects

we classify previous works that focus on emotive aspect as: Belief Models, Fuzzy Models, Semantic Web Models, and Game Theoretical Models.

Belief Models The basic idea of such models is to take the uncertainty of the user's feelings into account. In such models, trust relationships are considered as belief. Various techniques combining beliefs have been adopted. For example, the Dempster-Shafer theory (DST) was employed by Yu and Singh (2002). In their model, the information stored by an agent about direct interactions is a set of ratings that reflect the quality of these interactions. Josang (2002) used Subjective Logic arguing that subjective logic represents a belief calculus which can be used for analysis of trust networks (Josang et al. 2006). The trust value can be calculated as an instance of the opinion in the Subjective Logic (Yan and Holtmanns 2007). In these models, trust may be represented by a system holding a continuous value (crisp value) of trust, distrust and uncertainty (Abdessalem et al. 2010). The basic mathematical method of these models can be presented as Eq. (4):

$$Trust(x) + Distrust(x) + Uncertainty(x) = 1, x \in 2^{\theta}, x \neq \emptyset, \tag{4}$$

where θ is a set of possible states of a given system and x is a state in the power set of θ. Benefits of such models are considering the subjectivity and uncertainty of user's emotions (see Table 2). These two factors are the basis of belief formation about trusting other users. As we have shown in Table 2 in discussing potential challenges, using crisp value might cause inaccurate ratings. A user may find no or little difference between 3 and 4 values in a trust value scale of 5. Besides, these models only consider very recent interactions outcomes (ratings) to calculate trust value.

Fuzzy Models These models use linguistic terms instead of crisp value to represent trust. In such models, there are fuzzy membership functions which lead to calculate trust value

Table 2 Benefits and challenges of trust prediction models

	Main idea	Computation method	Benefits	Challenges
Belief models	(1) Users express their feelings about an interaction by crisp values (2) Users'feelings are used as basis for belief formation	Subjective logic	(1) Considering subjectivity in computations could bring trust value closer to user's feelings (2) Deriving subjectivity and uncertainty from user's feelings	(1) Considering only the most recent interactions (2) Users cannot express their feelings by crisp values
Fuzzy models	(1) Using linguistics terms to describe trust degree (2) Using Fuzzy membership functions	Fuzzy logic	(1) Compatibility with uncertain and ambiguous nature of trust (2) Linguistic terms are more understandable for humans	(1) Different conceptions of linguistic terms (2) Efficient fuzzy membership function is hard to define
Semantic web models	(1) Focusing on trusts semantic structure (2) The semantics of trust relationships is modeled using ontologies	Ontology	(1) Reusability of the available trust information in similar situations (2) Extensively used for recommender systems	(1) Implementation complexity will be high if the size of OSN increases
Game theoretical models	(1) Trying to model trust prediction as a trust game	Game theory	(1) Simple to understand	(1) Not suitable for large scale OSNs (2) Assuming actors are informed of the game
Flow models	(1) A participant's trust value increases as a function of incoming flow, and decreases as a function of outgoing flow	Network flow	(1) Suitable for computing global trust and reputation	(1) Ignoring user's interactions (2) Negative impact of normalization (3) Path dependence (4) Trust aggregation

Table 2 continued

	Main idea	Computation method	Benefits	Challenges
Spreading activation models	(1) Calculating trust for a set of source nodes and iteratively spreading that trust out to other nodes linked to the source nodes	Spreading activation networks	(1) Computing local trust (2) Using propagation trust for prediction	(1) Decaying trust value through chain could reach zero (2) Path dependence (3) Multiple paths or cycles between individuals (4) Varying the notion of trust for middle agents
Latent feature based models	(1) The underlying assumption is that the observed behavior of users is governed by latent features associated with both trustor and trustee	Matrix factorization	(1) Suitable for the situations where past interactions between two individuals are absent	(1) Strongly depends on existence of user's past interactions(with trustee or other similar agents)
Probabilistic models	(1) Updating PDFs with considering past trust values	Bayesian networks, ANNs	(1) Considering event sensitivity and time dependency of trust (2) Ability of assigning weight to past experiences	(1) Specifying correct intervals for updating trust values is difficult (2) Ignoring sudden changes in behaviors
Stochastic models	(1) Using Markov Decision Processes to model sequence of events and determining trust value with Stochastic Systems Theory	Sequence classification	(1) Modeling user's dynamic behavior pattern (2) Analyzing multi-person interactions (3) Estimating trust value in potential interactions	(1) It strongly depends on user's past behavior and outcome of interactions (2) High complexity for user-user trust prediction

from linguistic terms. The fuzzy membership functions for the linguistic terms such as low, medium, and high can be defined as depicted in Fig. 12.

Hence, the linguistic terms can also be used as trust values. Lesani and Montazeri (2009) use the Fuzzy Logic that provides rules for reasoning with fuzzy measures in OSNs. The Fuzzy Logic is suitable for trust prediction as it takes into account the uncertainties in expressions used to determine the trust (Abdessalem et al. 2010). Some trust models such as REGRET (Sabater and Sierra 2001) use fuzzy rules to reason about the trustworthiness of an agent's neighbors in providing honest opinions. For example, the degree of trustworthiness of the participants can be determined by demonstrating social relationships among agents in the form of fuzzy rules. In Bharadwaj and Al-Shamri (2009), a fuzzy computational model has been proposed which uses two fuzzy subsets [satisfied (Eq. (5))], unsatisfied (Eq. (6)). These subsets for partner a_i are defined as follows:

$$satisfied(a_i) = sat_{a_i}(e_k)|e_k \in H_i \tag{5}$$

$$unsatisfied(a_i) = unsat_{a_i}(e_k)|e_k \in H_i \tag{6}$$

where sat_{a_i} and $unsat_{a_i}$ are membership values of a_is ratings for e_k in the fuzzy subsets $satisfied(a_i)$ and $unsatisfied(a_i)$. Fuzzy membership functions are defined as Eq. (7) and Eq. (8):

$$sat_{a_i}(e_k) = \begin{cases} 0 & r_{a_j}^{e_k}(a_j) = z_* \\ \frac{(r_{a_j}^{e_k}(a_j) - z_*)}{z^* - z_*} & z_* < r_{a_j}^{e_k}(a_j) < z^* \\ 1 & r_{a_j}^{e_k}(a_j) = z^* \end{cases} \tag{7}$$

$$unsat_{a_i}(e_k) = 1 - sat_{a_i}(e_k) \tag{8}$$

where z_* and z^* are the minimum and maximum values for ratings.

Although Fuzzy models are usually preferred over Belief models in terms of simplicity and time complexity, a different interpretation of linguistic terms could cause an inaccurate trust prediction. Other trust prediction models usually combine with fuzzy models to satisfy the fuzziness property of trust and enhance prediction accuracy. Also defining an efficient fuzzy membership function is a challenging issue.

Semantic Web Models These models take a logical approach to trust formalization and as opposed to other models, mainly focus on trusts semantic structure and its logical conditions and effects (Tavakolifard 2012). The semantics of trust relationships are modeled using ontologies. In most cases, the user defines a list of trusted parties which is called Web of Trust. The semantic web of trust requires that users describe their beliefs about others. These beliefs are then used to predict trust values for all other users and available trust information is usable in similar situations (see Table 2). Anantharam et al. (2010) developed a general ontology of trust that is independent of any specific domain. In Golbeck (2006) an approach is introduced to integrate trust with annotations in Semantic Web systems. As a simple example, trust relationships (TR) are encoded in the form of triples, using RDF representation and OWL semantics (Boyd and Ellison 2008).

Such models are extensively used for recommender systems (FilmTrust Golbeck 2006), but if the size of the network grows, the implementation complexity will be high.

Game Theoretical Models These models aim to model trust prediction as a trust game (Sabater and Sierra 2005; Lumbreras and Gavald 2012). The game (see Fig. 13) involves two players, the trustor and the trustee (Buskens and Raub 2008). The trustor starts the game and he/she can choose between trusting or not trusting. If the trustor chooses not to trust, receives payoff P_1, while the trustee receives payoff P_2. If the trustor chooses

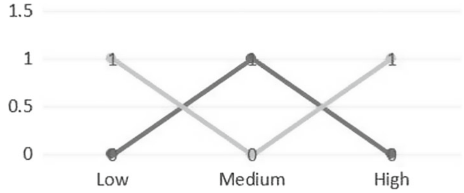


Fig. 12 Fuzzy membership functions of trust linguistic terms

to trust, the trustee chooses between honoring and abusing trust. If he/she honors trust, the payoffs for the trustor and the trustee are $R_i > P_i, i = 1, 2$. If he/she abuses trust, the trustor receives the payoff $S_1 < P_1$ and the trustee receives $T_2 > R_2$ (Vincent and Werner 2008).

In a large-scale OSN, the reliability of game theoretical models decreases due to high complexity of relations and interactions among agents. Furthermore, such models considered so far make the assumption that actors are completely informed on all features of the game. This assumption is often problematic for social interactions.

Cognition-based Approach This approach focuses on the characteristics of the trustee by using reputation and using OSN's properties such as social graph (Fig. 11). The main information sources are what the other agents said about the trustee and what can be concluded of social graph structure. This approach can be categorized into two main classes: Flow Models, Spreading activation Models.

- *Flow Models* These models take advantages of social graph and use incoming and outgoing flows to determine the reputation of each node (Laat et al. 2000). Agent's trust grows with the incoming flow and reduces with the outgoing flow [e.g., Google's PageRank (Yu and Singh 2002), Advogato (Levien and Aiken 1998), FlowTrust (Wang and Wu 2011), GFTrust (Jiang et al. 2015)]. As Fig. 14 shows the size of each circle is proportional to the total circles pointing it in PageRank.

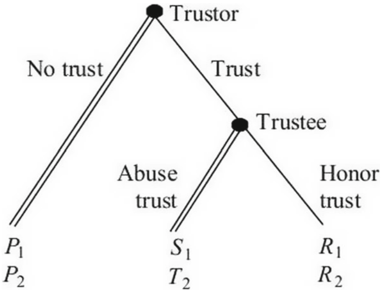


Fig. 13 The schematic of Trust Game (Vincent and Werner 2008)

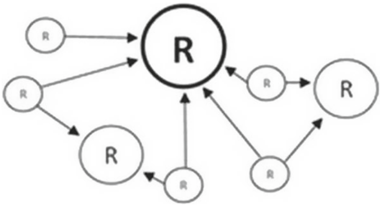


Fig. 14 The size of each circle is proportional to the total circles pointing it

Advogato identifies and cuts out untrusted nodes. The computation of Advogato is conducted according to trusted seeds; some nodes are taken as trusted seeds, then, the algorithm conducts a breath-first search on the graph; and according to the shortest distance from the target node to the seed, assigns each node a value. The FlowTrust approach considers network flow theory to model a trust network and stimulates the maximum amount of trust that can flow among agents in the trust network. GFTrust is a novel model that based on a modified network flow model with leakage. These models are simple to understand and implement, but using social graph flow and ignoring interactions between users could decrease the accuracy and attack resistance of such models. Avello and Brenes (2010) discussed how Flow Models which use graph structure and ranking algorithms can be gamed. They proposed a comparison of graph centrality algorithms in the case of recognizing spammers in Twitter. They apply a ranking algorithm to a pruned version of user graph (abusive users) and also desensitizing different variation of PageRank to become less sensitive to link abusing. Also, these models normalize trust value which could affect the final results. The most challenging issue of such models is path dependence and trust aggregation during a chain.

- *Spreading Activation Models* These models use graph properties for predicting trust. The trust prediction process is initiated by labeling a set of source nodes with weights or "activation" and then iteratively propagating or "spreading" that activation out to other nodes linked to the source nodes [e.g. Appleseed (Lausen and Ziegler 2005), TidalTrust (Golbeck 2005)]. These "weights" are trust values that decay as propagating through the network. These popular models simulate human comprehension through semantic memory (Quillian 1968). When direct observations are available, the trust value can be estimated, and then trust value of linked nodes can be calculated. When the source node does not have direct interaction with the target node, it can also predict trust through trust propagation as we have shown in Fig. 15.

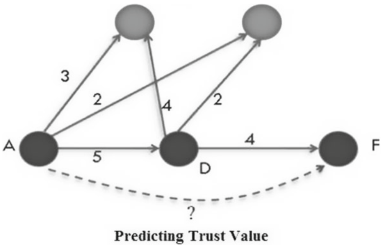
  An intuitive and very basic formula for calculating the transitive propagation of trust is represented in Eq. (9):

$$t_{ij}^{(h)} = \begin{cases} t_{ij} & if h = 1 \\ \sum_k t_{ik} t_{kj}^{(h-1)} & if h > 1 \end{cases} \tag{9}$$

  where h denotes the number of steps and the probability of i reaching j after h steps is seen as the probability of taking a single step to some vertex k and then taking $h - 1$ steps to j (Lumbreras and Gavald 2012).

  Golbeck (2005) and Golbeck and Hendler (2006) have proposed an extended-breadth-first search named TidalTrust, which performs trust inference through the strongest of shortest paths. The trust value between A and B is computed by Eq. (10):

Fig. 15 Predicting potential trust relationship using propagation trust



$$t_{AB} = \frac{\sum_{j \in N_A, t_{Aj} \geq max} t_{Aj} t_{jB}}{\sum_{j \in N_A, t_{Aj} \geq max} t_{Aj}} \tag{10}$$

where N_A is the neighbor set of A, and max is the threshold of being trustful (i.e., j is taken as trustful only if $t_A j \geq max$).

The very challenging problems in such models have shown in Table 2. These models strictly depend on the existence of trust path between source and target; if there is not a trust path between two agents, the trust value could not be predicted. If there are different paths between two individuals, using this method can give us different trust values. Furthermore, cycles in paths could bring some complexities to computations. Another problem with such models is that the notion of trust might vary for each agent-agent relationship and trust would only propagate through the edges of the same pattern. Also, decreasing trust value during chain may decay to zero.

Behavior-based Approach This approach focuses on the user's behaviors and exploits latent patterns in their interactions. Determining initial trust and tracking the trustee's behaviors and updating trust value according to his behaviors are main tasks in this approach (Fig. 11). Some models use statistical computations to understand user's behaviors (Adali 2013). Some other models exploit machine learning techniques (Massa and Avesani 2006); they consider trust prediction as a classification problem for computing and predicting trust based on the user's dynamic behaviors. If these algorithms manage to model efficiently what a trusted (or untrusted) interaction is, we can then use this to predict trustworthiness of a potential interaction (Bhuiyan et al. 2010). In the Behavior-based Approach, we have three major categories: Latent Feature-Based Models, Probabilistic Models, and Stochastic Models.

– *Latent Feature-Based Models* These models analyze the relationships between agents (Zheng et al. 2014) and try to predict trust from latent features in their behaviors. The underlying assumption is that the observed behavior of agents is controlled by latent features associated with both the trustor and the trustee. These models mainly rely on the agent's behavior pattern and similarity in his/her habits with other agents; and are trained based on the available data to predict the trust value between two non-adjacent (in social graph) participants. In this case, trust prediction model can use techniques such as matrix factorization, factorization machine, and deep learning based matrix factorization (Shuiguang et al. 2016).

  Matrix factorization model is an efficient mechanism for predicting missing values (Shuiguang et al. 2016). The premise behind such models is that there are few key features that affect agents interactions.The goal these models is to learn these latent features by minimizing Eq. (11):

$$\begin{aligned} L(R, P, Q) = \frac{1}{2} min_{P,Q} \sum_{i=1}^{m} \sum_{j=1}^{n} I_{ij} (R_{i,j} - P_i^T Q_j) \\ + \frac{\lambda_1}{2} \| P \|_F^2 + \frac{\lambda_2}{2} \| Q \|_F^2 \end{aligned} \tag{11}$$

  where $R \approx P^T Q$ and P and Q are feature matrix for all trustors and trustees, P_i refers to the feature vector of the trustor i and Q_j refers to the feature vector of the trustee j. $I_i j$ is the indicator function that equals 1 if agent i rated agent j and equals 0 otherwise. λ_1 and λ_2 are regularization terms to avoid model over-fitting. $\|.\|_F^2$ denotes the Frobenius norm.

Such models are commonly used for situations where past interactions between two individuals are absent. In this case, by analyzing the behaviors of the source and target agents with other agents, trust value can be derived. But if the past behaviors of the source and target agents with other agents do not exist, such models cannot predict trust without any hypothesis.

- *Probabilistic Models* In such models, trust prediction can be performed by Bayesian Networks and Neural Networks; which is the simplest case of a known structure and a fully observable Bayesian network (Yu and Singh 2002). Bayesian Networks statistically update the beta probability density functions (Katz and Golbeck 2006). The beta distribution can be expressed using the gamma function as Eq. (12):

$$Beta(\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1 - p)^{\beta-1} \tag{12}$$

Here $p \in [0, 1]$ is a probability variable, and $\alpha, \beta > 0$. This function shows the relative likelihood of the values for p, given the parameters α and β. The probability expectation of the beta distribution is computed by Eq. (13):

$$E(p) = \frac{\alpha}{\alpha + \beta} \tag{13}$$

Recent studies have shown that these approaches fail to effectively detect dynamic behavior patterns compared to stochastic models (see challenges in Table 2), because these models do not assume the weight of the current behavior. This is due to the underlying Bayesian framework, which assumes that the behavior of agents can be approximated by a fixed probability distribution. Since agents may change their behavior over time, this static modeling is not realistic. Another problem with such models is the lack of time component (Moe et al. 2009). Some early attempts regarding this issue extended the popular beta distribution-based trust models by adopting the forgetting factor (Josang and Ismail 2002; Teacy et al. 2006).

An artificial neural network (ANN)-based trust prediction model has been proposed in Azadeh et al. (2014). In this model linguistic expressions of trust values and the reliability of recommendations are taken into account; Z-numbers, introduced in Zadeth (2011), are used to convert qualitative expressions to real numbers; and then ANN is applied to predict trust values in the future.

However, there are a few disadvantages limiting ANN. The initialization and network topology design rely on the experience of a designer. ANN-based models are susceptible to over-fitting and hard to converge to the global optimal solution (Zheng 2015).

- *Stochastic Models* In these models, events are modeled by Markov decision processes and trust is computed using stochastic system theory. In this case, Hidden Markov Models (HMMs) are used for modeling the dynamic behavior of the agents. The works in Moe et al. (2008) and Malik et al. (2009) demonstrate how HMM-based trust models are applied to distinct application scenarios. In Moe et al. (2008) and ElSalamouny et al. (2010), a trust model is developed to help the trustor makes decisions over time in a dynamic environment. In Liu and Datta (2012), a HMM-based context aware trust prediction model is proposed which considers interaction contextual information that helps to reflect immensely on the dynamic behavior or the intent of an agent.

As Fig. 16 shows, in such models, after feature vectors from interactions are extracted, they will be used by HMM as input observations. An HMM-based classifier will be trained for each pair of interacting participants by estimating π, A, B (HMM parameters) and

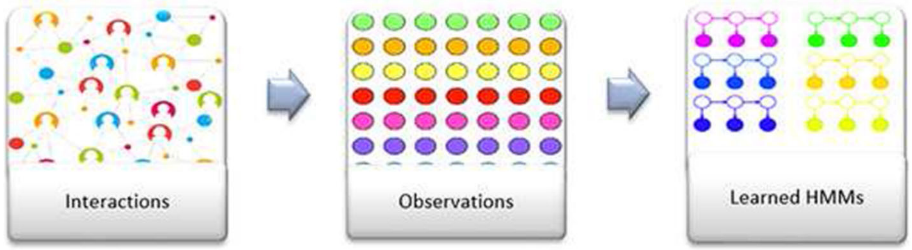


Fig. 16 Predicting potential trust relationship

when a new observation arrives, these parameters will be updated. The state transition matrix (A) will be used as trust transition probability.

As we have shown in Table 2, one problem that an HMM can solve is to determine the optimal state sequence for the given past states/observations. In fact, by using the state sequence, we are able to predict the trustee's trustworthiness based on the past interactions and observations (Yu and Singh 2002). If an agent treated in a trustworthy manner in the past and suddenly changes his behavior, stochastic models can detect these sudden changes. This is the most powerful benefit of stochastic models.

A summary of the proposed classification and related benefits and challenges is also represented in Table 2.

5.2 The proposed comparative criteria

For the purpose of presenting an efficient analysis of our proposed classification, we need to specify evaluation criteria which will be the basis of our comparison. Although such qualitative criteria are not measurable, understanding their importance could lead to an appropriate selection method for trust prediction and applying the predicted trust value in an effective manner. Although some of presented criteria are quantitative metrics, but we use them in a qualitative manner to propose an efficient comparison.

- *Coverage* It represents the ability of the algorithms to provide more predictions, i.e., the percentage of currently available links that can be predicted using the propagation method. Let P be the amount of source/target pairs that are predictable, and N be the total number of test pairs. Then, Coverage is represented by Eq. (14):

$$Coverage = \frac{P}{N} \tag{14}$$

- *Accuracy* It represents the ability to predict whether an agent will be trusted or not. Accuracy, itself is not a meaningful criterion for trust prediction, but some quantitative criteria which correspond to accuracy and have been used in other existing works, are based on prediction accuracy and classification accuracy (Liu et al. 2015).

  The metrics of MAE and RMSE represent how close the predictions are to the real trust values and refer to prediction accuracy; a smaller MAE or RMSE indicates a higher prediction accuracy.

  - MAE (Mean Absolute Error): The average of prediction error for all source-target nodes. It is calculated as Eq. (15):

$$MAE = \frac{1}{N}\sum_{k=1}^{N} |t_k - \hat{t_k}| \tag{15}$$

where t_k and $\hat{t_k}$ denote the real and predicted trust values, respectively.

- NMAE: To eliminate the effect of different ranges of trust values, we can normalize MAE. Normalized MAE (NMAE) is calculated as shown in Eq. (16):

$$NMAE = \frac{MAE}{|t_{max} - t_{min}|} \tag{16}$$

- RMSE (Root Mean Squared Error): The metric of RMSE is considered as an improvement of MAE (Massa and Avesani 2006), which is the root mean of squared prediction error. It is calculated by Eq. (17):

$$RMSE = \sqrt{\frac{1}{N}\sum_{k=1}^{N}(t_k - \hat{t_k})^2} \tag{17}$$

Precision and Recall are two metrics which refer to classification accuracy. Most studies have combined them into one metric which is called F-measure. A higher Precision and Recall indicates a higher classification accuracy.

- Precision: It represents the fraction of users who are predicted to be trusted and are really trusted ones. It can be calculated by Eq. (18):

$$Precision = \frac{A_t \cap B_t}{B_t} \tag{18}$$

  where A_t is the number of source/target pairs in which the source trusts the target directly, and B_t is the number of pairs in which the source trusts the target by the calculated trust.
- Recall: It represents the fraction of users who are really trusted and are successfully predicted. It tells us how complete the prediction is and is calculated by Eq. (19):

$$Recall = \frac{A_t \cap B_t}{A_t} \tag{19}$$

- F-measure: As Eq. (5.2) implies, by using the F-measure, the evaluation results would be more comparable.

$$F - measure = \frac{2.Precision.Recall}{Precision + Recall} \tag{20}$$

- AUC or AUROC: It represents the area under ROC curve and is a metric for binary classification. AUC is equal to the probability that a classifier will rank a randomly chosen positive instance higher than a randomly chosen negative one (Fawcett 2006). AUC is insensitive to imbalanced classes. In the case where class labels are mostly negative or mostly positive, a classifier that always outputs 0 or 1, respectively, will achieve high accuracy. In terms of AUC, it will score 0.5. For this reason, AUC is a better metric for classification performance.

– *Attack Resistance* It represents the level of vulnerability of the model to attacks. Unfortunately, this criterion is often ignored in trust prediction models. In trust prediction models, an attack can be a penetration of a foreign agent leading to a miscalculation in prediction. Trust prediction models could be an attractive target for attackers and scientists have identified various trust system attacks such as bad mouth attack, on-off attack, Sybil attack, Playbook. Further details about such attacks are provided in Sun and Liu (2006), Tavakolifard (2012).

- *Scalability* This parameter mainly depicts the relationship between changing OSN size and OSN load in dealing with the trust relationship. With the growth of OSN size, if the calculation complexity remains low, it means higher scalability. Specifically, a trust model with lower time complexity, lower space complexity, and a more efficient transmission pattern has a higher level of scalability.
- *Subjectivity* It represents the extent of considering the user's personal feelings and intellectual backgrounds in computations. In most presented models, subjectivity has been considered using the user's ratings.
- *Fuzziness* It represents the extent of considering trust ambiguity. Two factors refer to the fuzziness: uncertainty, inaccuracy. A proper trust model should take into account these concepts in trust establishing and measurement.
- *Recency* It represents the extent of involving the time parameter into trust predictions. The time parameter is an essential parameter in any trust prediction model and indicates the freshness of information. Older information should have less impact on calculations. In Keung and Griffiths (2008) recency is computed as trust decays over a fewer number of recent interactions between two entities. Similarly, in Huynh et al. (2006) a recency function is estimated to rate trust evidence as Eq. (21):

$$Recency(t_k, t) = e^{-\frac{t-t_k}{\lambda}} \tag{21}$$

  t is the current time and t_k is the time when evidence k is recorded. The parameter λ is to rate recency to scale time values (Cho et al. 2015).
- *Event-sensitivity* It represents the extent of considering more important events in trust prediction. An efficient trust model should consider more weight for important events and less weight for irrelevant events.

5.3 Analytical assessment of frequent trust prediction models

The most important component of TP-TA framework is the assessment of our proposed classification which analyses the extent to which comparative criteria proposed in the previous section are satisfied. In this section, we assess the classification of trust prediction models. The qualitative comparison of the proposed approaches is a guide to understand their superiority over one another. Table 3 shows assessment of trust prediction models with regard to trust aspects.

- *Coverage* Models in the Cognition-based approach have a high level of coverage; because the more propagation of trust value occur through a chain, the more predictable pairs would be available. As we have shown in Table 3, Spreading Activation Models have the highest level of coverage as the basis of such models is predicting trust values by spreading source trust value through chains (Lausen and Ziegler 2005) and using trust inference techniques such as Graph Search algorithms and Tree Search algorithms which use trust aggregation methods through the identified paths to finally infer the trust from the source to the target (Lesani and Montazeri 2009). If a trusted path exists between the source and the target, then trust value of this pair is predictable. The coverage of Flow models is lower that Spreading Activation Models, because these models are based on in-degree and out-degree of nodes and the trust value of an isolated node cannot be predicted.

  All models in Emotion-based category have low coverage; because they need an explanation of user's feelings and if there is no such information, trust cannot be predicted.

Table 3 Assessment of trust prediction models

Approach	Model	Coverage	Accuracy	Attack resistance	Scalability	Subjectivity	Fuzziness	Recency	Event-sensitivity
Emotion-based	Belief models	Low	Low	Very low	Medium	High	Very high	Low	Medium
Emotion-based	Fuzzy models	Low	Medium	Low	Low	Very high	Very high	Low	Medium
Emotion-based	Semantic web models	Low	Medium	Medium	Very high	High	Medium	Low	Medium
Emotion-based	Game theoretical models	Low	Medium	Medium	Medium	High	Medium	Low	Medium
Cognition-based	Flow models	High	Medium	Low	Medium	Low	Low	Low	Low
Cognition-based	Spreading Activation Models	Very high	Low	Medium	Low	Low	Low	Low	Low
Behavior-based	Latent feature based models	Medium	High	Medium	High	Medium	Low	Low	Medium
Behavior-based	Probabilistic models	Low	High	Medium	High	Medium	Low	Medium	Medium
Behavior-based	Stochastic models	Low	Very high	Very high	High	Medium	High	Very high	Very high

In the behavior-based approach, because of their interaction-based nature, if we do not consider any prior hypothesis about trust propagation, the coverage level will be low. Although the interaction based nature of behavior-based approach is different from propagation trust techniques that take advantage of social graph and trust network, if the network is interpreted as a Bayesian Network or a Markov chain, we can apply a random walk model considering trusts as probabilities and, in general, considering trust as the probability for source to reach target (Lumbreras and Gavald 2012). But without considering random walk in such models, Latent feature-based models have a medium level of coverage, because they can predict trust value between two agents that have no interaction record with each other based on their interaction history with other similar agents. Probabilistic and Stochastic models are poor in coverage and if there is no interaction between two agents, trust value cannot be predicted without considering any hypothesis.

Accuracy In Spreading Activation models, accuracy will decrease when walking along a path from the source to the target (Golbeck 2004). We should be careful about such models which take advantage of graph properties. In such models, accuracy decreases through a chain. If the model has predicted trust value for the source node with high accuracy, it does not mean that this obtained accuracy level is valid for middle nodes or the target node. Also trust value will decay during the chain and at last will equal zero. Therefore, we assign low-level accuracy to such models. Flow models have medium level of accuracy, because they only rely on social graph properties without considering the validity of users'behaviors.

Emotion-based approaches deeply depend on users'ratings and explicit feedbacks which can cause some miscalculation (See challenges in Attack Resistance). We assign a medium level of accuracy to such models. However, in Belief models, because of using crisp value, users may not be able to express their feelings correctly. Therefore, Belief models are weak in accuracy.

Behavior-based approaches are efficient in accuracy because of their interaction-based nature and considering past behaviors, outcome of such models are closer to reality. In such models, accuracy can be evaluated by classification accuracy metrics which were introduced in the previous section. Stochastic models have the highest level of accuracy, because there is a trained model for each pair of participants that considers features and characteristics of that unique relationship.

Attack Resistance Emotion-based approaches which use the user's rating are extremely vulnerable to attacks related to rating systems because users sometimes try to game the system. First of all, the subjectivity of the user's ratings can cause some major problems, such as false feedbacks which means that users provide incorrect ratings. In Tavakolifard (2012) this type of attacks are categorized as dishonest and unfair reports and collusion. The former category is the result of the low cost of submitting online ratings or anonymity of raters. The latter category occurs when multiple agents boost each other reputation or conspire against another agent. Sybil-based attacks are another category to which emotion-based approach is vulnerable (Sun and Liu 2006). In this case, malicious user acquires multiple accounts to create phantom ratings. To overcome this problem, semantic web models take advantage of the Web of Trust and, thus, the effect of the attackers will be limited based on the expense of social interactions.

In the cognition-based approach the most important attack that could happen is related to trust propagation via incredible parties during a chain. Attackers could penetrate into a chain to boost trust value of a conspired target node. In this case, during trust propagation, considering the reputation and history of recommenders could be an effective solution.

In Flow models, users maybe use non-conventional methods to boost their in-coming flow, such as paying money to another users to follow them.

Behavior-based approaches could be attacked by sudden misbehaviors of agents. In this case, Playbook attack could happen. A playbook is a sequence of actions that maximize profits of a participant according to certain criteria (Tavakolifard 2012). A typical example is to act honestly over a period to gain a high reputation, and then subsequently misuse of the gained reputation. Stochastic models have the power to detect such sudden changes in behaviors.

Scalability Emotion-based approaches have efficient scalability. Such models can use distributed approaches which each node computes trust value of its neighboring nodes. Semantic web models have the highest level of scalability, because of using web of trust. For all models which are categorized under cognition-based approaches that use graph properties to predict trust value, scalability will be low as the size of network grows and these models are not reliable in huge OSNs. Such models are effective when used as local solutions.

On the other hand, scalability of behavior-based approaches is high, because of using distributed computation for each node of the network and computations do not depend on the size of network and deeply depend on the number of interactions. If the number of interactions grows, the dimensions of feature vectors will grow, but it can be handled by efficient feature engineering methods (feature extraction, feature selection etc.).

Subjectivity As we mentioned in Sect. 5.1, Belief and Fuzzy models consider user's personal feelings. Also Semantic web models and game theoretical models consider user's personal feeling by involving them in choosing their trusted partners, explicitly. So the emotion-based approach has the highest level of subjectivity. In Fuzzy models, because of using linguistic terms for rating, users express their feelings in a better way. In the cognition-based approach, subjectivity is low because such models propagate trust from the source to the target without considering the middle nodes'personal feelings.

Although behavior-based models can raise their level of subjectivity by involving users rating as their basic input, but the focus of such models is users'implicit behaviors, not users'personal feelings. However, in Probabilistic models like beta models, ratings are considered as the main source of information. Thus, because these models can be integrated with ratings, we assign them a medium level of subjectivity.

Fuzziness As we showed in Table 3, Fuzzy models have the highest level of fuzziness. In fuzzy logic an agent can be partially trusted, in the sense that he is 80% honest and 20% dishonest. So uncertainty and the blurry nature of trust are reflected in an efficient way. Belief models consider uncertainty into account, too.

Also, Behavior-based approaches such as Stochastic models assume an underlying state, and observations are uncertain and we have an uncertainty reported in Moe et al. (2009). But in Probabilistic models and Latent feature based models, the new state of an agent is certain with some probability. This means that we know exact which state will be the new state, according to the probability of each state. So such models have a low level of fuzziness.

To enhance the level of fuzziness, other models are usually combined with fuzzy models. There are some efforts in combining Spreading Activation models with fuzzy models.

Recency The highest level of recency belongs to behavior-based approaches because in such models users'behaviors are analyzed over time. Stochastic models are efficient in considering the time and freshness of information in computations. In such models, time component is associated with the underlying state transition process. Probabilistic models

with the forgetting factor have a medium level because they consider time decay using the forgetting factor, but it is a fixed factor which decays over time by a fixed measure.
All other models are static trust models which do not consider time in computations. Some of these models consider fixed intervals to update trust values dynamically and they need to re-run trust computation in specified intervals; but choosing a sufficient interval is a challenging issue.
Event-sensitivity This criterion is satisfied by stochastic models because such models perform better when it comes to the detection of changes in the behavior of agents over time. Probabilistic models are easily understandable and verifiable but they are not weighted toward the current behavior. This is due to the underlying Bayesian framework, which assumes that the behavior of agents can be approximated by a fixed probability distribution. Since agents may change their behavior over time, this static modeling is not realistic (Moe et al. 2009). But in such models, we can assign more weights to important events to increase their impact. Also in Emotion-based approach, we can suppose that users consider important events in their ratings. However, these models have not any consideration for this criterion.
Other models are not sensitive to important events without considering any hypothesis.

6 Discussion

In this section we discuss the benefits and implications of our proposed framework; we also highlight the potential future works and directions in the field of Trust Prediction in OSNs which can be concluded from our proposed framework. The main implications of our framework can be categorized as follows:

- *Model Selection* One of the most important applications of TP-TA is the provision of selecting the efficient approach at different levels of details for use in different applications. In this case, we deal with the selection of a Trust Prediction model with respect to the type of OSN. In this level, the process of model selection is closely related to the type of OSN and its definition of relationships among agents. First, we should specify which conceptual approach is more suitable for the target OSN by answering these questions:

  - What is the main entity of the target OSN?
  - What is the main goal of trust relationships in the target OSN?
  - Which trust approach of TP-TA focuses on the main entity of the target OSN?

  For instance, in task-oriented OSNs, the task is the main entity and doing a task in the desired way is the main goal. According to TP-TA, the behavior-based approach is more efficient because it focuses on interactions and the quality of interactions. Alternatively, in advice-provider OSNs, the main entity is the advice and the goal is providing advice by reliable agents. In this regard, the cognitive approach is more applicable, because users trust reliable advisers; it means the characteristics of the trustee are more important. By contrast, in friendship-oriented OSNs, the main entity is users' profile and the goal is socializing. In such networks, accepting friendship requests strongly depend on the trustor's taste and the emotion-based approach is more suitable.
  In the next step, we should specify which one of the technical models is suitable for the target network by considering pros and cons summarized in Table 2 and assessment criteria presented in Table 3. As an instance, if in the task-oriented OSN, there are numerous of interactions among the users and sudden changes in user's behaviors are

important, we can choose Stochastic Models. Alternatively, if the rate of interactions among users is low, we can use Latent Feature-based Models to extend existing trust values to similar users. In advice-provider OSNs, we can use Flow Models if we want to estimate rank and trustworthiness of the advisors or Spreading Activation Models to introduce trusted advisors to other users. In friendship-oriented OSNs, if a rating system exists in the target OSN, we can use Belief Models (in the case of numeric ratings) or Fuzzy Models (in the case of linguistic ratings) to calculate trust values. If there are labels for describing the relationships by users (e.g., family, close friends, co-works, etc) we can choose Semantic Web Models. If there is an awarding system, we can take advantage of Game Theoretical Models.

We attempted to illustrate the benefits of our proposed framework in model selection, but mapping the type of OSNs to our classification is a broad study which is beyond the goal of this paper and can be a future research work.

- *Model Combination* TP-TA could be a source for understanding how models can be combined to mitigate the shortcomings of each other. Considering the main ideas in Table 2, we can understand which models are compatible with each other and from Table 3 we can determine the combination of which models can enhance their low or medium degrees. In this case, combination of models with the same approach or models with different approaches can be discussed. For instance, as we have shown in Table 3, all models in the cognition-based approach have a sufficient degree of coverage, but emotion-based or behavior-based approaches are weak in this regard. To enhance the level of coverage of these approaches, a new model can be proposed which combines one of the weak models with one of the models in the cognitive-based approach. For example, the combination of Fuzzy Models or Belief Models with Flow Models can result in a new model which considers the trustor's feelings as well as the trustee's characteristics (e.g., reputation). In this way, the low subjectivity of the Cognition-based approach can be enhanced with the high subjectivity of the Emotion-based approach, and the low level of coverage of the Emotion-based approach can be enhanced by the Cognition-based approach.

  Also, the combination of Stochastic Models and Spreading Activation Models can be a future research work; where the initial trust value is calculated by a trained HMM and then propagates to predict new trust value during a chain of users. In this way, the high level accuracy of HMM can enhance the low level accuracy of Spreading Activation Models, and the low coverage of HMM can be enhanced by the high level coverage of Spreading Activation Models.

  Another instance is the combination of Belief Models or Fuzzy Models with one of the models in the behavior-based approach. Here, the trustor rates the trustee after a direct interaction (the interaction has a weight itself) and such rating can be taken into account while evaluating an interaction.

  In fact, Table 3 could be a valuable source for merging different models to propose a new and enhanced model which we believe can lead to new research works.
- *Elimination of challenges* TP-TA provides the ability to eliminate or mitigate the defects and challenges of each approach and also each model by the divide and conquer method. In fact, the subject of predicting trust in OSNs is divided into three major parts (the conceptual level of our classification). In this level, we deal with the concepts of trust and consequently the existing challenges of trust prediction on the conceptual level. For instance, as we have stated in Sect. 5.3, all Emotion-based models are faced with the big challenge of low attack resistance. In fact, this approach is vulnerable in many ways. Also Cognition-based approaches are based on network structure which can cause some

cost and complexity of implementations. Behavior-based approaches strongly depend on interactions between users on OSNs, but these approaches cannot recognize family, friends or other real world relationships. In such situations if interactions between users do not exist, this approach fails to predict a trust value close to reality.
In the next step, we divide each approach into the technical models. In this level, we should deal with the technical challenges of each model. We believe Tables 2 and 3 are shortcuts for understanding the challenges of trust prediction. Finding solutions for all the challenges summarized in Tables 2 and 3 can be taken by future work.

– *New ideas* TP-TA also can lead to generating new ideas in the field of Trust Prediction in OSN. We believe understanding trust prediction models and their main ideas, pros and cons could be a good help to know which technique is a trend in this area or which points need to be improved. As an instance, with a quick look at Table 2 we can find out Stochastic Models are powerful and have a potential to be improved in future. Also, we can find out that trust prediction models lack some trending subjects such as deep learning and unsupervised feature learning. This can opens up a completely new area of research work in the field of Trust Prediction because all the existing works in this field only consider static features and they have feature engineering step.

We believe by closely studying Tables 2 and 3, new directions and possibly improvements can be made in the field of Trust Prediction in OSNs which we attempted to briefly describe some examples above.

7 Conclusion

In this paper, we proposed a coherent analytical assessment framework for trust prediction techniques with respect to a trust aspect, called TP-TA. The main purpose of TP-TA is analyzing different trust prediction models for the efficient selection of trust prediction models based on the type of target OSN, since the selection of a trust prediction model for specific OSN is related to the type of OSN that is affected by trust aspects. We provided a state-of-the-art account of existing methods with a new angle: First, by closely studying existing trust prediction methods, we categorized them into major trust aspects and clarifying the extent of focusing on trust aspects and describing their basic ideas, prospects and challenges of them. Then, we defined a set of common criteria to compare them in a qualitative manner. Finally, by analyzing the proposed classification in the level of satisfying each criterion, we presented a guideline for the efficient selection of trust prediction models.

References

Abdessalem T, Cautis B, Souhli A (2010) Trust management in social networks. ISICIL

Adali MT (2013) Context in networks. Springer, New York

Adali S, Escriva R, Goldberg MK, Hayvanovych M, Magdon-Ismail M, Szymanski BK, Wallace WA, Williams GT (2010) Measuring behavioral trust in social networks. In: 2010 IEEE international conference on intelligence and security informatics (ISI), Vancouver, BC, Canada

Alunkal BK (2003) Grid Eigen Trust: a framework for computing reputation in grids. In: Master's thesis, Illinois Institute of Technology

Anantharam P, Henson CA, Thirunarayan K (2010) Trust model for semantic sensor and social networks: a preliminary report. In: Proceedings of the IEEE national aerospace and electronics conference

Avello DD, Brenes DJ (2010) Overcoming Spammers in Twitter—a tale of five algorithms. In: Conference on information retrieval

Azadeh A, Kokabi R, Saberi M, Hussain FK, Hussain OK (2014) Trust prediction using z-numbers and artificial neural networks. In: IEEE international conference on fuzzy systems, Beijing, China

Beatty P, Reay I, Dick S, Miller J (2011) Consumer trust in e-commerce web sites: a meta-study. ACM Comput Surv (CSUR) 43(3). doi:10.1145/1922649.1922651

Bharadwaj KK, Al-Shamri MYH (2009) Fuzzy computational models for trust and reputation systems. Electron Commer Res Appl 8(1):37–47

Bhuiyan T, Josang A, Xu Y (2010) Trust and reputation management in web-based social network. In: Usmani Z-U-H (ed) Web intelligence and intelligent agents. InTech, Rijeka, pp 207–232

Boyd DM, Ellison NB (2008) Social network sites: definition, history, and scholarship. J Comput Mediat Commun 13(1):210–230

Brandtzaeg PB, Lders M, Skjetne JH (2010) Too many Facebook friends? content sharing and sociability versus the need for privacy in social network sites. Int J Hum Comput Interact 26:1006–1030

Buskens V, Raub W (2008) Rational choice research on social dilemmas: EMBEDDEDNESS EFFECTS ON TRUST. In: Handbook of rational choice social research

Castelfranchi C (2009) A non-reductionist approach to trust. In: Golbeck J (ed) Computing with social trust. Springer, London Human-Computer Interaction Series

Cho J-H, Chan K, Adali S (2015) A survey on trust modeling. ACM Comput Surv 48(2). doi:10.1145/2815595

ElSalamouny E, Sassone V, Nielsen M (2010) HMM-based trust model. In: Dimitrakos T, Martinelli F, Ryan PYA, Schneider S (eds) Formal aspects in security and trust. Springer, Berlin

Fang H, Bao Y, Zhang J (2014) Leveraging decomposed trust in probabilistic matrix factorization for effective recommendation. In: Proceeding AAAI'14 proceedings of the twenty-eighth AAAI conference on artificial intelligence. AAAI Press, Qubec, Canada, pp 30–36

Fawcett T (2006) An introduction to ROC analysis. Pattern Recogn Lett 27:861–874

Golbeck HJ (2004) Accuracy of metrics for inferring trust and reputation in semantic web-based social networks. In: Motta E (ed) Engineering knowledge in the age of the semantic web. Springer, Berlin

Golbeck J (2005) Computing and applying trust in web-based social networks, Ph.D. dissertation. University of Maryland, College Park

Golbeck J (2006) Combining provenance with trust in social networks for semantic web content filtering. In: Provenance and annotation of data, pp 101–108

Golbeck J, Hendler J (2006) Inferring binary trust relationships in Web-based social networks. ACM Trans Internet Technol 6(4):497–529

Grabner-Kruter S, Bitter S (2013) Trust in online social networks: a multifaceted perspective. Forum Soc Econ 44(1):48–68

Gray E, Seigneur J-M, Chen Y, Jensen C (2003) Trust propagation in small worlds. In: International conference on trust management, pp 239–254

Guha R, Kumar R, Raghavan P, Tomkins A (2004) Propagation of trust and distrust. In: Proceedings of the 2005 ACM workshop on privacy in the electronic society, New York, NY, USA

Huang Z, Ruj S, Cavenaghi MA, Stojmenovic M, Nayak A (2014) A social network approach to trust management in VANETs. Peer-to-Peer Netw Appl 7(3):229–242

Huynh TD, Jennings NR, Shadbolt NR (2006) An integrated trust and reputation model for open multi-agent systems. Auton Agents Multi-Agent Syst 13(2):119–154

Jiang W, Wang G, Bhuiyan MZA, Wu J (2016) Understanding graph-based trust evaluation in online social networks: methodologies and challenges. ACM Comput Surv 49(1). doi:10.1145/2906151

Jiang W, Wu J, Li F, Wang G, Zheng H (2015) Trust evaluation in online social networks using generalized network flow. IEEE Trans Comput 65(3):952–963

Josang A (2002) A logic for uncertain probabilities. Int J Uncertain Fuzziness Knowl Based Syst 9(3):279–311

Josang A, Hayward R, Pope S (2006) Trust network analysis with subjective logic. In Proceeding ACSC '06 proceedings of the 29th Australasian computer science conference, Darlinghurst, Australia

Josang A, Ismail R (2002) The beta reputation system. In 15th Bled electronic commerce conference. Bled, Slovenia

Josang A, Ismail R, Boyd C (2007) A survey of trust and reputation systems for online service provision. Decis Support Syst 43(2):618–644

Josang A, Pope S (2005) Semantic constraints for trust transitivity. In: Proceedings of the 2nd Asia-Pacific conference on conceptual modelling, Darlinghurst, Australia

Katz Y, Golbeck J (2006) Using social network-based trust for default reasoning on the web. J Web Semant

Keung S, Griffiths N (2008) Using recency and relevance to assess trust and reputation. In: Proceedings of the AISB symposium on behavior regulation in multi-agent systems (BRMAS08), Aberdeen, UK

Laat CD, Gross G, Gommans L, Vollbrecht J, Spence D (2000) Generic AAA architecture. Network working group

Lausen C, Ziegler G (2005) Propagation models for trust and distrust in social networks. Inf Syst Front 7(4–5):337–358

Lesani M, Montazeri N (2009) Fuzzy trust aggregation and personalized trust inference in virtual social networks. Comput Intell 25(2):51–83

Levien R, Aiken A (1998) Attack-resistant trust metrics for public key certification. In: In Proceedings of the 7th USENIX security symposium

Liu X, Datta A, Lim E-P (2015) Computational trust models and machine learning. CRC Press, Chapman and Hall, Boca Raton

Liu X, Datta A (2012) Modeling context aware dynamic trust using hidden Markov model. In: Proceedings of the twenty-sixth AAAI conference on artificial intelligence

Lumbreras A, Gavald R (2012) Applying trust metrics based on user interactions to recommendation in social networks. In: International conference on advances in social networks analysis and mining, IEEE Computer Society Washington, DC, USA

Malik Z, Akbar I, Bouguettaya A (2009) Web services reputation assessment using a hidden Markov model. In: Proceedings of the 7th international joint conference on service-oriented computing, Stockholm, Sweden

Marsh SP (1994) Formalising trust as a computational concept. University of Stirling, Stirling

Massa P, Avesani P (2006) Trust-aware bootstrapping of recommender systems. In: Proceedings of 2006 ECAI workshop on recommender systems

Ma S, Wolfson O, Lin J (2011) A survey on trust management for intelligent transportation. In: Proceedings of the 4th ACM SIGSPATIAL international workshop on computational transportation science, New York, NY, USA

Minhas UF, Zhang J, Tran T, Cohen R (2010) Intelligent Agents in mobile vehicular ad-hoc networks: leveraging trust modeling based on direct experience with incentives for honesty. In: IEEE/WIC/ACM international conference on web intelligence and intelligent agent technology

Moe MEG, Tavakolifard M, Knapskog SJ (2008) Learning trust in dynamic multiagent environments using HMMs. In: Proceedings of The 13th Nordic workshop on secure IT systems, Copenhagen, Denmark

Moe ME, Helvik BE, Knapskog SJ (2008) TSR: Trust-based secure manet routing using HMMs. In: Proceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks, Vancouver, Canada

Moe M, Helvik BE, Knapskog S (2009) Comparison of the beta and the hidden markov models of trust in dynamic environments. International Federation for Information Processing

Nepal S, Sherchan W, Bouguettaya A (2010) A behaviour-based trust model for service web. In: Service-oriented computing and applications (SOCA)

Pourkazemi M, Keyvanpour M (2010) A survey on community detection methods based on the nature of social networks. In 3rd International eConference on computer and knowledge engineering (ICCKE)

Quillian R (1968) Semantic memory. Semantic information processing

Rousseau DM, Sitkin SB, Burt RS, Camerer C (1998) Not so different after all: a cross-discipline view of trust. Acad Manag Rev 23(3):393–404

Sabater J, Sierra C (2001) REGRET: reputation in gregarious societies. In: Proceedings of the 5th international conference on autonomous agents, Montreal, Quebec, Canada, pp 194–195

Sabater J, Sierra C (2005) Review on computational trust and reputation models. Artif Intell Rev

Sherchan W, Nepal S, Paris C (2013) A survey of trust in social networks. ACM Comput Surv 45(4):47

Shuiguang D, Huang Longtao X, Xindong GW, Zhaohui W (2016) On deep learning for trust-aware recommendations in social networks. IEEE Trans Neural Netw Learn Syst PP(99):1–14

Sun YL, Liu KJR (2006) A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks. In: PROCEEDINGS—IEEE INFOCOM

Sztompka P (1999) Trust: a sociological theory. Cambridge University Press, Cambridge

Tavakolifard M (2012) On some challenges for online trust and reputation systems, PhD Thesis

Teacy WTL, Patel J, Jennings NR, Luck M (2006) TRAVOS: trust and reputation in the context of inaccurate information sources. Auton Agents Multi-Agent Syst 12(2):183–198

Victor P, Cornelis C, De Cock M (2011) Trust networks for recommender systems. Springer, Berlin

Vincent B, Werner R (2008) Rational choice research on social dilemmas: embeddedness effects on trust. In: Nee V, Wittek R (eds) Handbook of rational choice social research. Russell Sage, New York

Wang G, Wu J (2011) FlowTrust: trust inference with network flows. Front Comput Sci 5(2):181–194

Xia W, Cao M, Johansson KH (2015) Structural balance and opinion separation in trust-mistrust social networks. IEEE Trans Control Netw Syst 3(1):46–56

Yan Z, Holtmanns S (2007) Trust modeling and management: from social trust to digital trust. In: Computer security privacy and politics: current issues, challenges and solutions, IGI Global

Yan Z, Kantola R, Shi G, Zhang P (2013) Unwanted content control via trust management in pervasive social networking. In: 2013 12th IEEE international conference on trust, security and privacy in computing and communications

Yu B, Singh M (2002) An evidential model of distributed reputation management. In: Proceedings of the first international joint conference on Autonomous agents and multiagent systems

Zadeth LA (2011) A note on z-numbers. Int J Inf Sci 181(14):2923–2932

Zheng X (2015) Trust prediction in online social networks, PhD Thesis, Macquarie University

Zheng X, Wang Y, Orgun MA, Liu G, Zhang H (2014) Social context-aware trust prediction in social networks. In: Basu S, Pautasso C, Zhang L, Fu X (eds) Service-oriented computing. Springer, Berlin