Knowledge-Based Systems 106 (2016) 150–163

Contents lists available at ScienceDirect

Knowledge-Based Systems

journal homepage: www.elsevier.com/locate/knosys

A survey of trust management systems for online social communities – Trust modeling, trust inference and attacks

Yefeng Ruan*, Arjan Durresi

Indiana University Purdue University Indianapolis, Department of Computer and Information Science, Indianapolis, IN 46202 USA

ARTICLE INFO

Article history:
Received 14 September 2015
Revised 19 May 2016
Accepted 21 May 2016
Available online 25 May 2016

Keywords:
Online trust
Trust management
Online social communities
Attack

ABSTRACT

Trust can help participants in online social communities to make decisions; however, it is a challenge for systems to map trust into computational models because of its subjective properties. Also, many online social communities are sparsely connected. Therefore, it is necessary to introduce mechanisms which can infer indirect trust among participants who are not directly connected. We provide a survey of existing trust management systems for online social communities. We also list four types of attacks, and analyze existing systems' vulnerabilities. Compared with previous surveys, our survey takes trust modeling, trust inference, and attacks into account. Although there are several survey papers about global trust/reputation related attacks, the main contribution of this paper is that we consider trust inference and potential local trust related attacks.

1. Introduction

Due to the development of the Internet and computer-based devices, especially smart phones, people are now moving at least part of their social activities to online environments. In the last few years, many online social networks, such as Facebook and Twitter, have spread out around the world. Participants in such kinds of social networks can have a large number of claimed friends. Some of them may be well known, while some are not. One possible way to deal with this problem is to differentiate them by using trust metrics. Huberman et al. [1] differentiate "claimed friends" from "real friends" in Twitter by counting the number of interactive tweets that two users post toward each other. Besides social networks, many other online applications also exhibit social properties, for example e-commerce [2–4], like eBay [5], Amazon and Epinions [6,7], and P2P file sharing networks [8,9]. In this paper, we call them online social communities in which participants can be users, agents, devices, or others.

We have seen that trust plays an extremely important role in online social communities, as well as in people's lives; however, there are some challenges in applying trust in online social communities [10]. First of all, we have to represent trust in a computational model. Trust is not easy to model in a computational way because of its subjective property [11]. Also, it cannot be applied directly in online social communities due to different features that online social communities have from traditional social networks [12]. For example in real life, people only have a limited number of friends to evaluate, but this number explodes in online social communities. On Facebook and Twitter, users can have thousands of friends. Apart from this, in real life, trust is developed slowly over time, based on face-to-face social experiences; however, this is very difficult in online social communities due to the large number of potential friends. Therefore, trust in online social communities must be computational such that it can be processed by computers [11,12]. The difficulty is that trust is a subjective concept, and it has different meanings in different fields and applications [13,14]. For example, in Amazon, participants use stars to represent to what extent they think others' reviews are useful. While in other cases, such as in P2P networks, trust measures the quality of downloaded files, downloading speed, and so on [8,15]. Therefore, trust modeling should be dependent on applications or scenarios. In the remainder of this paper, we use the term trust modeling to denote how to represent trust in a computational way.

Besides trust modeling, another challenge is how to infer indirect trust information among two unconnected participants. In many online communities, only a small number of participants are directly connected, compared with the potential number of pairs of participants. Many works have shown that online communities are sparsely connected [1,7,12,16,17]. Therefore, it is urgent to introduce mechanisms that can be used to infer indirect trust among participants who are not directly connected. Such type of framework is described as "Friend of a Friend (FOAF)" in [18]. Basically,

* Corresponding author.
E-mail addresses: yefruan@cs.iupui.edu (Y. Ruan), durresi@cs.iupui.edu (A. Durresi).

http://dx.doi.org/10.1016/j.knosys.2016.05.042
0950-7051/

trust propagates along chains; however, how to propagate trust is still an open debate. Both general and application specific mechanisms are proposed by many researchers in this field [19–28].

In this paper, we use the term trust management systems to denote the systems dealing with how to represent, infer, and use trust. We provide a survey for existing trust management systems used in various online social communities. We mainly focus on two challenges – trust modeling and trust inference. Although there are several survey papers about computational trust [29–31] and global trust/reputation related attacks [32–34], the main contribution of this paper includes:

- We provide a survey for trust inference problem, which takes into account inferring indirect trust relationship for not directly connected participants.
- We provide a survey for four types of local trust related attacks, and analyze existing schemes' vulnerabilities to them.

The rest of this paper is organized as follows: in Section 2, we investigate various definitions of trust, and introduce some related works. In Section 3, we review how existing works deal with the first challenge – trust modeling. In Section 4, we illustrate the second challenge – trust inference, and survey several existing schemes. In Section 5, we illustrate four types of attacks in trust management systems. In Section 6, we analyze existing schemes' vulnerabilities to four types of attacks. In Section 7, we conclude the paper.

2. Background and related works

2.1. Definition of trust

Trust is a relationship existing between two participants. In this paper, we use truster and trustee to denote them. Trustee is the participant being evaluated by the truster. For example, when we say *A* trusts *B, A* is the truster and *B* is the trustee.

Trust is studied and used in a number of disciplines, such as sociology, psychology, economics, computer science, and so on. As a result, there are many definitions for trust and no general consensus has been achieved so far [35,36]. Among them, one of the recent summarized definition is given by [36]:

> "Trust is the willingness of the trustor (evaluator) to take risk based on a subjective belief that a trustee (evaluatee) will exhibit reliable behavior to maximize the trustor's interest under uncertainty (e.g., ambiguity due to conflicting evidence and/or ignorance caused by complete lack of evidence) of a given situation based on the cognitive assessment of past experience with the trustee" [36].

In this definition, trust is explained as the probability of performing a specific action. In the field of computer science, besides probability, there are many other representations of trust, such as entropy [37,38], similarity [39–41], and so on. We will see different types of representations of trust in the following.

Trust can be classified based on various criteria. In [42], McKnight classified it into three categories: impersonal/structural trust, dispositional trust, and personal/interpersonal trust. Impersonal/structural trust is determined by institutional properties rather than by participants themselves. Dispositional trust represents participants' bias trust preferences. Personal/interpersonal is the participant-to-participant trust relationship. Among them, personal/interpersonal trust has attracted ample attention from researchers. In this paper, we mainly focus on personal/interpersonal trust. For simplicity, we call it trust in the following. Trust can be further divided into functional trust and recommender trust based on the types of behaviors [43]. Functional trust describes how trustworthy a person is when implementing functions, e.g. how good Alice is as a doctor. Recommender trust measures how reliable a person's recommendations are, e.g. how reliable Alice's recommendations are about doctors.

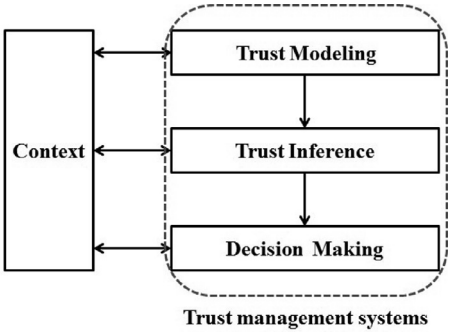

Fig. 1. Framework of trust management systems.

Trust has many properties, such as subjective, dynamic, asymmetric, context dependent, transitive, composable, and so on [11,13,29]. Similar to its definition, different applications highlight different aspects of its properties.

2.2. Trust management systems

Trust management systems are designed to help participants to make better decisions based on trust information. According to Ries et al. [31], trust management systems can be divided into three parts: trust modeling, trust management and decision making. Trust modeling mainly deals with how to represent trust relationships in computational models, and trust management is used to describe how to collect evidence and to do risk evaluation. Decision making is another important and complicated field, and can even be treated separately [31]. As trust modeling and trust management, together, mainly deal with how to represent trust in computational models using available raw data, we incorporate them together and use trust modeling to represent them. Apart from them, we also include trust inference into trust management systems as it is a very important component for trust management systems to work more intelligently and efficiently. Trust inference uses direct trust information among participants to infer indirect trust information. In this paper, we mainly focus on trust modeling and trust inference.

We represent the framework of trust management systems in Fig. 1. All three phases are dependent on context or applications, especially trust modeling and decision making. For example, depending on the type of available data, systems would map appropriately the raw data into defined trust metrics. Similarly, depending on context, such as risk, systems might use different methods to aggregate and filter trust, in trust inference. Finally, in decision making, for example, systems might apply different levels of trust thresholds when participants select a doctor for an important surgery, compared with when they decide whether or not to watch a movie. Furthermore, the three above phases are interrelated. So, the accuracy of trust inference, and its corresponding level of support in decision making will depend on the availability and granularity of raw trust data from the field.

2.3. Related works

As online social communities are becoming more popular, there are also more works investigating trust relationships in this field of computer science. As a result, there are several survey papers in this field.

Sabaster and Sierra [29] provide a survey for computational trust and reputation models. It also discusses their properties. Grabner-KrÃ¤uter and Kaluscha [30] provide a survey for trust in the field of E-commerce from economists' points of view. Ries et al. [31] mainly focuses on the classification of trust modeling. It reviews how trust is represented and what is the semantic meaning of trust in different systems, e.g. rating, probability, fuzzy logic, etc. Jøsang provided a survey for trust's categories and semantic meanings in [5]. Besides trust, he also investigated another trust related concept – reputation. Furthermore, he gave some application examples in the paper, such as Amazon, Epinions, and Slashdot. Golbeck provided a comprehensive survey on trust modeling in [14]. It classifies trust based on its objects. Massa reviewed some challenges in trust management systems in [44]. It includes how to represent trust in various types of online systems. Also, it mentions a few identity related attacks, such as fake identities and multiple identities. Sherchan et al. [13] provide a survey for trust in web-based social networks. It shows how trust is defined in different disciplines and also gives its definition for web-based social networks. It mainly focuses on data collection, trust evaluation and trust dissemination. Cho et al. [36] provide a survey for trust modeling in complex, composite networks. It includes four layers of trust: communication trust, information trust, social trust and cognitive trust. It reviews trust from multiple disciplines' points of view, such as sociology and psychology.

There are also a few works discussing the relationship between trust and security. Ruohomaa and Kutvonen [32] discusse the concept of trust in the field of computer security. It mainly focuses on determining initial trust metrics and updating trust metrics based on observed behaviors. It also describes how trust can be used in computer security applications, such as authentication, intrusion detection, and so on. Similar to [32,33] also discusses the potential usage of trust in E-commerce to counter attacks. Cho et al.[45] combine social trust and quality-of-service trust for Mobile Ad Hoc Networks (MANETs). It also investigates several potential attacks; however, attacks discussed are application-oriented. They are specifically related to MANETs, such as routing loop attacks, replay attacks, and so on. Wang et al. [46] list several requirements of different security problems and potential attacks in trust management systems, but without examining existing systems' vulnerabilities. Hoffman et al. [34] provide a survey about potential attacks and defense techniques in reputation (global trust) systems. While in this paper, we focus on attacks related with local trust.

Although there are several surveys existing for trust management systems [29–31], they rarely investigated trust inference. Many of them considered that trust management systems can be used to detect malicious users, but without considering trust management systems themselves can be the targets of attacks. Some surveys only considered attacks in specific applications or environments, such as [32,33,45,47]. Therefore, in this paper we provide a comprehensive survey for trust management systems for online social communities, which consider both trust inference and potential attacks.

3. Trust modeling

In this section, we review how existing works deal with the first challenge we mentioned – trust modeling. As indicated in [31], trust modeling deals with how to represent trust in computational models using available raw data. In details, it includes the metrics they used to represent trust, how many dimensions they have, what is the trust information source, and what are the semantic meanings of trust.

3.1. Trust metrics

3.1.1. Trust scaling

As we stated, in order for computers to be able to process trust, it must be represented in a computational way. Metrics can be either numerical or categorical. Trust is always represented by numerical values. In the literature, there are two types of numerical values, discrete and continuous values, used to quantitatively measure trust. Discrete values come from raw data, such as ratings, scaled metrics, and so on [43]. Continuous values are also often used in trust management systems. For example, probability based, or similarity based trust metrics [8,39], are always continuous. Besides numerical values, trust can also be represented by intervals [48,49].

- Binary discrete values. One of the most straightforward ways for the truster to express her/his opinion about the trustee is to use binary metrics – trust or distrust. In many applications, it is also the final goal for the truster to make a binary decision. There is a large number of research works that model trust relations using binary metrics [50–53].
- Multinomial discrete values. Although binary metrics are easy for participants to use and understand, in some cases, trust and distrust may not be sufficient to represent the truster's opinions. With more scaled metrics, like "very trust", "trust", "distrust" and "very distrust", participants can evaluate others more accurately because they have more options [36].
- Continuous value. Continuous value is another popular way to represent trust. Due to the semantic meaning of many applications, such as probability and belief, continuous value is a straightforward way to represent trust. Many works belong to this category [12,23,54–58].
- Interval. Instead of representing trust using a single value, some works use intervals to represent trust, as in many cases trust is uncertain. Interval is used by many fuzzy logic-based trust models. Examples include [48,49].

3.1.2. Trust dimension

In many works [8,20,21,26,53,59], trust is represented by a single value; however, as trust has many properties, in some cases, two or more parameters are used to represent trust. In this section, we use the term trust dimension to denote the number of parameters that are used.

- Separated distrust. In systems that use a single trust value, distrust is considered as the complement of trust. In these systems, high value represents trustworthy, while low value represents untrustworthy [12,20]. However, this is not always true [36]. Guha et al. [50] and Golbeck and Hendler [60] separate distrust from trust and treat them independently. Besides distrust, Marsh and Dibben [61] introduce untrust and mistrust into the system.
- Time stamps. As trust is dynamic, it is important for researchers to consider time stamps for trust status. By incorporating time stamps, trust can be updated and used to defend certain attacks [55]. Example considering time stamps include [27,55,62,63].
- Context. Trust is context dependent [36]. The trustee may exhibit different trust degrees or trustworthiness given various types of contexts. For example, a good babysitter is not necessary a good car repairer. Therefore, many works are context-aware [27,43,56,64–66].
- Confidence/certainty. Confidence or certainty is used in trust management systems to measure to what extent the truster is certain about her/his trust assessment. It is considered as an important additional metric in many trust management systems [12,60,67–69]. Therefore, we illustrate it in more details in Section 3.3.

Furthermore, there are many works that include other dimensions. For example, Subjective Logic [70] uses relative atomicity to denote the percentage of uncertainty contributing to the expected belief.

3.1.3. Trust source

According to Sherchan et al. [13], trust can be derived from three sources: attitude, experience and behavior.

- Explicit attitude. Attitude represents the truster's opinion towards the trustee. It can be either trust/like/positive or distrust/dislike/negative. Although Sherchan et al. [13] indicate that attitude can be derived from interactions or experiences, in this paper we only consider explicit attitude information. For example, in Epinions.com, users express either trust or distrust attitude [6]. Also, for those systems assuming trust values are directly and explicitly available, such as [24,50,52,53,60], we consider them as using explicit attitude.
- Evidence/feedback/experience. When the truster interacts or makes transactions with the trustee, the truster is able to evaluate the trustee's performance. For example, satisfactory transactions and unsatisfactory transactions are used to measure trust in [8]. Evidence is used in systems which consider belief theory [23,69–71]. Also, rating is widely used in many systems to calculate trust [12,21,22,72]. Note that although these systems all use evidence/feedback/experience, their semantic meanings are different. We illustrate this in Section 3.2.
- Behavior. Trust can also be evaluated based on behaviors [13]. In [73] and [74], authors used reply, forward and retweet behaviors to capture trust information. Adali et al. [75] also use communication behaviors to measure trust. Besides these application specific behaviors, we also consider similarity as one of the behaviors. Similarity measure how similar two agents are, for example, their purchasing behaviors [76,77], common communities they join [78], profile similarity [57,79], and so on.

3.2. Semantic meanings of trust

Trust has different semantic meanings in different scenarios and applications. We discuss some existing schemes' semantic meanings of trust in the following. Also, we note that some systems, such as [20,50,80], simply assume trust values are extant without digging into their semantic meanings.

3.2.1. Evidence or experience based trust

In many cases, participants build up trust based on their prior evidence or experiences. The truster assesses all experiences she/he had with the trustee. Given those assessments of evidence, there are still multiple methods to model trust.

- Probability. As pointed out by Gambetta [81], trust can be expressed by the probability that the trustee will behave as the truster expects. One of the most popular theories used in trust management systems is Dempster-Shafer Theory (DST). Based on DST, Jøsang et al. proposed a model which takes binary evidence as input and computes trust values [70], as well as many other researchers [23,69,71,82,83]. Sun et al. [37] calculate trust based on probability's entropy.
- Mean. It is a straightforward way to calculate the mean of evidence as the trust value. For example, Zhang and Durresi [12] use the average ratings (from 1 star to 5 starts) as trust values.
- Mode. Given the set of evidence, instead of calculating the mean value, an alternative way is to find the mode of the discrete evidence, such as [43].
- Difference. Trust value can also be calculated by the difference between positive and negative evidence. Kamvar et al. [8] calculate the difference ($\#positive\ evidence - \#negative\ evidence$) first, and then for each participant p it normalizes local trust values with the summation of p's all outgoing trust values.

3.2.2. Application specific behavior based trust

When calculating trust, some specific types of behaviors are especially important. Here we distinguish behaviors from evidence although evidence can be considered as one specific type of behavior.

- Conversational behaviors. For example, Ruan et al. [74] consider in Twitter that conversation and forwarding are two factors to determine trust. If two participants have balanced long term conversations, most likely they trust each other. Similarly, they assume that if the truster forwards the trustee's messages very frequently, it means that the truster trusts the trustee. In [84], authors consider retweet and favorite as two trust-related behaviors in Twitter. Also, Adali et al. [75] use conversational behaviors, such as conversation duration and frequency, to measure trust.

3.2.3. Similarity based trust

Similarity was first used in collaborative filtering (CF) recommender systems. They make recommendations based on the similarity between participants or items [76,85]. Similarity can be an additional metric in trust management systems in determining trust [2,3,56,77,79]. The assumption is that, for participants who are similar with each other, most likely they also trust each other.

3.2.4. Reputation

Reputation is different from local trust. We consider it as one type of trust, as in many systems it is considered in the decision making stage. Reputation is widely used in many systems, such as e-commerce systems [86] and P2P networks [87,88]. Instead of asserting trust metrics for each pair of participants, each participant only has a unique value which represents how the whole community (centralized [82]) or part of the community (distributed [64,89]) evaluates this participant. Furthermore, it can affect agents' personal/interpersonal trust. Examples of reputation systems include [64,87–96].

3.2.5. Fuzzy logic based trust

Because of trust's nondeterministic property, many works adopted fuzzy logic to model trust. Unlike traditional logic metrics, fuzzy logic is among completely true and completely false [97]. Schemes using fuzzy logic to represent trust include [98–101].

3.2.6. Comprehensive trust

Trust is a summarization of complicated human behaviors, and it can be affected by many factors. Because of its human-related properties, besides the above mentioned factors, some researchers tried to take into account several other factors when computing trust values [102]. For example, Marsh defined trust from the disciplines of psychology, sociology, biology and economics, and stated many rational principles and rules, which are adopted by later works [11]. In [57], Zhan and Fang concluded that trust is dependent on three components: profile similarity, information reliability and social opinions. Besides direct connections, [62] also takes into account users' susceptibility and others' contagious influence. In [78], friendship, social contact (based on frequently visited locations) and community of interest contribute to the trust. Trust in [27] is divided into interpersonal trust and impersonal trust. It further considers four aspects (benevolence, competence, integrity and predictability) for interpersonal trust. ReputationPro [65] uses

a tree-like structure to compute trust. Hao et al. [103] calculate trust from four aspects: prestige, familiarity, similarity and risk of trust.

From the above description, we can see that there exist several different representations and meanings for trust depending on scenarios and applications. It is very difficult to say which one is the best, or which one can outperform another, as the validation is also application dependent.

3.3. Trust and confidence/certainty

With the development of trust management systems, many researchers found that trust value itself is not enough to manage trust relationships. In many schemes [12,43,67,82], researchers introduced another important concept – confidence (or certainty) into trust management systems. Confidence is used to measure how certain the truster is about her/his trust views about the trustee.

By using confidence, the truster can distinguish distrusted participants from unknown participants. Participants can have different levels of confidence even though they have the same level of trust. For instance, although both distrusted participants and unknown participants have very low trust levels, the confidence is different. Typically, distrusted participants have very high confidence due to their previous bad behaviors. While unknown participants have very low confidence since they are new in the communities.

Another important role of confidence is to imply the number of evidence or experiences based on which trust is evaluated. Confidence will increase as the total number of evidence increases. Confidence is also an important factor in the decision making stage. For example, when we are faced with high risk events, we may choose to cooperate with participants that have both high trust levels and high confidence.

Like trust, there are also several ways to represent confidence. In [70], Jøsang et al. used a multi-tuple to represent belief, disbelief and uncertainty, which sum up to 1.0. In this case, uncertainty is dependent on belief and disbelief. Confidence in [12] is determined based on the uncertainty in measurement theory. There are also several works that use similarity based confidence [22,104], as well as fuzzy theory [105].

In Table 1, we list some schemes and their corresponding representations, semantic meanings, as well as trust dimensions for trust. Also, we examine each scheme to see if they support trust inference (properties of transitive and composable).

4. Trust inference

The goal of trust management systems is to provide participants with trust information and help them to make decisions; however, in many online communities, only a limited number of participants are directly connected. Therefore, using existing direct trust is not sufficient. It is urgent to introduce trust management systems which can infer indirect trust by making use of direct trust links [51]. In the field of computer science, there are many proposed trust inference schemes. Some of them were designed for specific applications, while some were proposed for general purposes. We review some existing schemes in this section.

There exist two very important operators in the trust inference schemes: transitivity/concatenation operator and aggregation operator [70,106]. Transitivity operator is used to calculate trust propagation in a single chain. It helps participants to evaluate others even though they do not have any prior direct experiences. Aggregation operator is used for combining parallel trust paths between the truster and the trustee in case that there exist more than one trust path between them.

In the following, we classify some existing schemes based on the methods they used to calculate trust transitivity and aggregation. We list the methods they used to propagate and aggregate trust separately; however, trust transitivity and aggregation in some schemes, such as the matrix factorization category, are combined together.

4.1. Multiplication for transitivity and weighted mean of evidence for aggregation

4.1.1. Abdul-Rahman and Hailes

Abdul-Rahman and Hailes [43] divide trust into two categories: direct trust and recommender trust. Trust in this case has four discrete values: very trustworthy, trustworthy, untrustworthy and very untrustworthy. The truster maintains a set of prior experiences with the trustee. To determine the trust value, it returns the mode of four trust degrees. If there are more than one returned trust degrees, it assigns a uncertainty value. Furthermore, trust propagates through recommendations. The truster compares her/his own experiences with the recommender's suggestions and then adjusts the recommender trust accordingly. Experiences are aggregated by weighted mean, where weights are intermediary participants' recommender trust. Similarly, aggregated trust is the mode of four trust degrees.

4.1.2. Jøsang

In [70], Jøsang proposed a model called Subjective Logic that considers trust as a term of uncertain probability. Trust is represented in two spaces – opinion (or belief) space and evidence space. Following Dempster-Shafer Theory (DST), Jøsang defined four important parameters: belief (b), disbelief (d), uncertainty (u) and relative atomicity (a) in the opinion space, and $b+d+u=1$. In the evidence space, it focuses on binary events: positive evidence (represented by r) and negative evidence (represented by s). The posterior probability of binary events is represented by Beta distribution. Furthermore, there exists a mapping between the evidence space and the opinion space.

It uses discounting and consensus operators to propagate and aggregate trust correspondingly. Intermediary participants' recommendations about the trustee are discounted by their trustworthiness. In trust transitivity, both belief and disbelief decrease, while uncertainty increases. This makes sense in real life that uncertainty increases when introducing more intermediary participants within a chain. Consensus operator adds evidence together from multiple parallel trust paths and converts them into the opinion space. Jøsang extended [70] to a new version, which uses conditional belief reasoning in [107]. As we will see later, Subjective Logic is adopted by many other researchers in this field.

4.1.3. Sabestian

In Sabestian's model, which is called CertainTrust [71], trust is also represented in two spaces. Human Trust Interface (HTI) contains trust and certainty. The second representation focuses on the evidence domain. To determine certainty, it sets a maximal number (E_m) of expected evidence for each context. Certainty increases when evidence increases; however, it does not increase linearly. In the beginning, few evidence can make certainty increase a lot. While there are already a large amount of evidence, certainty increases not as fast as before. When the number of evidence is greater than or equal to E_m, certainty is normalized to 1. In the evidence domain, similar to [70], it also uses Beta distribution to model the posterior probability of binary events. There exists a map between the above two representations. Trust is equal to the mode of Beta distribution.

Table 1
Representations, semantic meanings and properties of trust.

Schemes	Trust scaling	Semantic meaning	Trust dimension	Trust inference
Marsh [11]	Continuous $[-1, 1)$	Comprehensive	CT, TS	No
Abdul-Rahman and Hailes [43]	Discrete (multinomial)	Evidence based (mode)	CT, CF	Yes
Jøsang [70]	Continuous [0, 1]	Evidence (probability)	DT, CF	Yes
Falcone, Pezzulo et al. [98]	Continuous $[-1, 1]$	Fuzzy logic	NA	NA
Kamvar, Schlosser et al. [8]	Continuous [0, 1]	Evidence (difference)	NA	Yes
Guha and Kumar [50]	Discrete (binary)	NA	DT	Yes
Xiong and Liu [64]	Continuous [0, 1]	Reputation	CT, CF	Yes
Golbeck [21]	Continuous [0, 1]	NA	CT	Yes
Sun, Yu et al. [37]	Continuous $[-1, 1]$	Evidence (entropy)	TS, CT	Yes
Massa and Avesani [20]	Continuous [0, 1]	NA	NA	Yes
Sabestian [71]	Continuous [0, 1]	Evidence (probability)	CT, CF	Yes
Wang and Singh [67]	Continuous [0, 1]	Evidence (probability)	DT, CF	Yes
Uddin, Zulkernine et al. [56]	Continuous [0, 1]	Similarity	TS, CT, CF	Yes
Adali, Escriva et al. [75]	Continuous [0, 1]	Behavior	TS	Yes
Leskkovec, Huttenlocher et al. [52]	Discrete (binary)	NA	NA	NA
Nepal, Sherchan et al. [63]	Continuous [0, 1]	Comprehensive	TS, CT	No
Victor, Cornelis et al. [60]	Continuous [0, 1]	NA	DT, CF	Yes
Zhan and Fang [57]	Continuous [0, 1]	Comprehensive	NA	No
Liu, Wang et al. [80]	Continuous [0, 1]	Comprehensive	NA	Yes
Wang and Wu [68]	Continuous [0, 1]	Evidence (probability)	CF	Yes
O'Doherty, Jouili et al. [26]	Continuous	Comprehensive	NA	No
Zhang and Durresi [12]	Continuous [0, 1]	Evidence (mean)	CF	Yes
Kant and Bharadwaj [99]	Continuous [0, 1]	Fuzzy logic	DT	Yes
Fang, Zhang et al. [62]	Continuous [0, 1]	Comprehensive	TS,CT	Yes
Chen, Guo et al. [78]	Continuous [0, 1]	Comprehensive	NA	Yes
Shakeri and Bafghi [49]	Interval	Evidence	CF	Yes
Liu, Yang et al. [69]	Continuous [0, 1]	Evidence (probability)	DT, CF	Yes
Zhang and Mao [53]	Discrete (binary)	NA	NA	Yes
Aref and Tran [101]	Continuous	Fuzzy logic	TS	No
Fang, Guo et al. [27]	Continuous [0, 1]	Comprehensive	TS, CT	Yes

For trust dimension, DT = Separated Distrust, TS = Time stamp, CT = Context, CF = Confidence/certainty, NA = Not available.

For trust transitivity and aggregation, two operators – consensus and discounting, are defined. Both of the operators first calculate in the evidence domain and then convert to HTI.

4.1.4. Wang and Singh

As in [70], Wang and Singh also represented trust in the evidence space and the belief space; however they defined certainty differently in [67]. It has an another important parameter – evidence conflict, which represents the ratio of positive evidence to the total evidence. In this definition, certainty is dependent on both the conflict ratio and the number of evidence.

Operators for trust transitivity and aggregation are similar to [70]. Apart from transitivity and aggregation operators, authors added another operator – selection, in [108]. Selection operator is used to select reliable trust paths among multiple trust paths between the truster and the trustee.

4.1.5. Liu, Yang et al.

Apart from belief, disbelief and uncertainty used in Subjective Logic, ASSESS-TRUST [69] incorporates another metric: posterior uncertainty. Relatively, it calls uncertainty defined in Subjective Logic the prior uncertainty. In the evidence space, it includes three types of evidence: positive, neutral and negative evidence. Mapping exists between the opinion space and the evidence space using Dirichlet distribution. Aggregation operator has the same idea as in Subjective Logic, except for extending from binary evidence to tri-nary evidence. In the transitivity operator, instead of transferring evidence to the prior uncertainty, it transfers evidence to neutral evidence, which in turn increases the posterior uncertainty. In a recursive manner, ASSESS-TRUST calculates trust from the truster to the trustee using transitivity and aggregation operator.

4.2. Multiplication for transitivity and weighted mean of trust values for aggregation

4.2.1. Kamvar, Schlosser et al.

EigenTrust [8] is mainly designed for P2P file sharing systems. It measures trust based on the number of satisfied and unsatisfied experiences. The truster's outgoing trust is normalized by the summation of all her/his outgoing links. It uses multiplication to propagate trust and aggregates trust by weighted mean, where weights are intermediary participants' trust.

4.2.2. Xiong and Liu

PeerTrust [64] is another trust management system designed for P2P networks. It uses reputation based trust metrics. Also, it allows participants to propagate recommendations to their neighbors. It uses weighted mean to aggregate trust; however, weights are dependent on personalized similarity. Similarity is determined by two participants' feedback, number of transactions, credibility of feedback, transaction context factor and community context factor.

4.2.3. Golbeck 2005

In [21], Golbeck proposed a trust management system – TidalTrust. It uses weighted mean to combine trust from multiple trust paths. In order to improve accuracy, it only takes recommendations from trustworthy neighbors, which means that their trust is greater than a threshold. Also, it sets a limitation for path lengths because Golbeck believed that inferred trust from a long path is not as reliable as that from a short path. It is evaluated in a social network called FilmTrust.

4.2.4. Sun, Yu et al.

Sun et al. proposed a trust model in [37] based on entropy – an important measure of uncertainty in information theory. p denotes the probability that the trustee will perform the action as the

truster expected. Trust is defined by the entropy of p. Trust is positive when $p > 0.5$, and it is negative when $p < 0.5$. When $p = 0.5$, trust is equal to 0, which means that the truster is uncertain about the trustee. It uses weighted mean and only considers recommendations from trustworthy intermediary participants (whose trust is positive) to aggregate trust.

4.2.5. Massa and Avesani

In [20], Massa and Avesani proposed a trust model called MoleTrust. It takes two steps to propagate and aggregate trust. In the first step, it takes input the truster, trust network and trust propagation horizon, and outputs a modified trust network. Here the input trust network includes the whole community. Trust propagation horizon limits the maximum number of hops (path length). In the second step, it infers indirect trust within the modified trust network (the outcome of the first step). It computes indirect trust in an iterative way, in which the trustworthiness of a node at distance k only depends on the nodes at distance $k-1$. The inferred trust is the weighted mean of all the accepted incoming links. When selecting incoming links, only those links whose trust is greater than, or equal to, a threshold will be taken into account.

4.2.6. Liu, Wang et al.

Liu et al. [109] uses the product of links' trust as the prior probability for trust inference in a single path. The posterior probability is adjusted by the Bayesian network. It considers social intimacy degree and recommendation role in the Bayesian network. When there are multiple trust paths between the truster and the trustee, it uses weighted mean to combine them, where weights are assigned according to social intimacy degree and recommendation role and adjusted by the Bayesian network as well. Apart from social intimacy degree and recommendation role, preference similarity is also taken into account in [80].

4.2.7. Zhang and Durresi

In [12], Zhang and Durresi proposed a trust management system based on measurement theory. It considers social interactions among participants as "measurements". Trust (impression) is similar to "measured value of object", and confidence represents the certainty of a "measurement". So in this model, confidence is related to the "error" in measurement theory. For trust transitivity, there are three principles in [12]. Guided by these principles, it uses multiplication to calculate trust transitivity and weighted mean to calculate trust aggregation. In their work, weights are trust paths' confidence.

4.3. Selection for transitivity and average for aggregation

4.3.1. Golbeck 2006

Golbeck proposed two algorithms – Rounding algorithm and Nonrounding algorithm, to infer indirect trust for a binary trust network [51]. Participants in [51] are labeled as either "trusted" or "not trusted". Good participants refer to those agreeing with the truster (source) with a certain probability, while bad participant refers to those who are always opposed to the truster. To infer indirect trust, the truster directly takes her/his good neighbors' recommendations, without discounting them. When there are multiple paths, the truster averages the recommendations. In the Rounding algorithm, all the participants round the average ratings to {0,1} in each step. While in the Non-rounding algorithm, all intermediary participants hold continuous average values, and only the truster does the final rounding.

4.4. Matrix propagation

4.4.1. Guha and Kumar

Guha and Kumar took both trust and distrust into account in their work [50]. It is the first work which considers the propagation of distrust. Compared with trust, propagation of distrust is much more complicated. It defines two matrices, matrix of trust T and matrix of distrust D. Matrix of belief B can have two formats, $B = T$ or $B = T - D$, depending on applications. It includes four atomic propagation operators in this scheme: direct propagation (B), Co-citation (B^TB), transpose trust (B^T) and trust coupling (BB^T). Direct propagation means that if A trusts B and B also trusts C, then A trusts C as well. If $A1$ trusts $B1$ and $B2$, and $A2$ trusts $B1$, it is probable that $A2$ also trusts $B2$ because $A1$ and $A2$ have the same views on $B1$. This is defined as Co-citation. Transpose trust means that if A trusts B, then B may trust A back. In trust coupling, if B and C both trust D, and A trusts B, it implies that A may trust C. These four operators are combined together forming a propagation matrix $C_{(B,a)} = a_1B + a_2B^TB + a_3B^T + a_4BB^T$, where a_1, a_2, a_3, a_4 are the weights of four operators.

There are three models to propagate trust: trust only, one-step distrust and propagated distrust. The trust only model ignores distrust, the one-step distrust model discounts judgments made by distrusted neighbors, and both trust and distrust can be propagated in the propagated distrust model. All three models have a limitation on the chains' length.

4.4.2. Zhang and Mao

In [53], trust is propagated similar to [50]. But it reduces to two atomic operators: transposition and forwarding, as other two (co-citation and coupling) can be deduced from them. Instead of propagate trust deterministically, it assumes transposition and forwarding happen with some probabilities. It also assumes that there can be a probability that two random participants can be connected without through transposition and forwarding. Given all the information, the posterior probability of inferred links can be calculated. It uses the factor graph to represent the dependence between variables (links) and functions (probability functions). In such a way it calculates the posterior probability using belief propagation algorithm (also known as sum-product algorithm). Final prediction of binary trust is based on the sorting of the probabilities.

4.5. t-norm for transitivity and weighted mean for aggregation

4.5.1. Victor, Cornelis et al.

In [60], Patricia Victor et al. derived trust from bi-lattices. In the definition, similar to [50], trust includes both trust degree (t) and distrust degree (d), which are independent with each other. It means that even if the trust degree is very high, e.g. $t = 0.9$, distrust degree can also be very high, e.g. $d = 0.9$. In this case, $t + d > 1.0$. It indicates information contradictory and knowledge defect $kd(t, d) = |1 - t - d|$. Certainty can be derived from knowledge defect.

With regard to trust propagation, it only uses trustworthy paths, as distrust information is very complicated and difficult to use. Unlike others, instead of proposing one trust propagation operator, it lists several operators. It uses weighted mean to aggregate trust from parallel trust paths. It also proposes several operators based on how to set weight for each path.

4.5.2. Wang and Wu

Wang and Wu [68] compute trust and certainty by collecting evidence and using Dempster–Shafer Theory as in [70]; however it considers multi-dimensional evidence and trust. It also proposes several selection strategies, such as selecting primitive dimensions

and subsets. To propagate trust, it uses the parameterized family of Frank t-norm [110], in which discounting rate is controlled by the input parameters. Multiple trust paths are combined by weighted mean, where weights are derived from certainty of trust paths. It also tackles the problems caused by shared links (links shared by two or more paths between the truster and the trustee) and crossing links (links cross two paths) in trust networks.

4.5.3. Verbiest, Cornelis et al.

Verbiest et al. [111] adapt the framework from [60]. It represents trust using bi-lattices approach; however, to aggregate multiple paths between the truster and the trustee, Verbiest et al. [111] uses weighted mean approach where weights are dependent on paths' length. As increasing paths' length can decrease inference's accuracy, it weights paths' influence based on the order of paths' length. Also, it proposes a dynamic horizon search strategy, in which it sets a global threshold for the length of path; however, when the shortest paths' length is less than the global threshold, it only considers those shortest paths. By incorporating paths' length into trust inference, it tries to optimize the trade-off between coverage and accuracy.

4.6. Multiplication for transitivity and maximum for aggregation

4.6.1. Zhao and Li

VectorTrust [112] provides a local trust management for P2P file sharing systems. It uses a single value to represent trust degree/level. To propagate trust, trust degrees/levels are multiplied together along the chains. And when there are more than two paths between the pair of users, it selects the most trustworthy path. Note that, only when the truster has no direct trust towards the trustee, indirect trust will be inferred and used.

4.6.2. Hao, Min et al.

MobiFuzzyTrust [103] models trust in a comprehensive way. It considers prestige-based trust, familiarity-based trust, similarity-based trust and risk, and combines them to calculate trust value; however, instead of using the numerical values, MobiFuzzyTrust represents trust with linguistic terms. Fuzzy membership functions are defined to convert trust from numerical values to linguistic terms. To infer indirect trust, it first multiplies numerical values. If there exist more than one path between the truster and the trustee, it chooses the path which has the maximum trust value. Finally, the numerical trust values are converted back to linguistic terms using the fuzzy membership functions.

4.7. Social theories bases method

4.7.1. Huang, Kimming et al.

In [113], Huang, Kimming et al. proposed a trust framework based on Probabilistic Soft Logic (PSL) [114]. It uses soft truth values as trust degrees. To infer indirect trust for unconnected truster and trustee, it follows two social theories – balance theory and status theory, and develops two rules correspondingly. Specifically, following balance theory, only triangles which contains one or three strong/positive links are considered as balanced. In status theory, if the truster trusts the trustee, it means that the trustee has higher status than the truster. Also, it takes reciprocation of trust into account as another rule for two social theories.

4.8. Machine learning based method

As machine learning becomes more popular, there are also many works using machine learning techniques to predict social links for online social communities [52,102,115–117]. In such types of works, each link is labeled as positive or negative. Kim and Song [118] combine behavior based methods, such as weighted mean and min-max aggregation, and machine learning method – reinforcement learning, together. In this paper, we mainly focus on trust management systems which are behavior based.

Table 2
Weights in weighted mean schemes.

Schemes	Weights
Abdul-Rahman and Hailes et al. [43]	Recommender trust
Jøsang [70]	Trusters' direct trust
Sabestian [71]	Product of trust and confidence
Wang and Singh [67]	Trusters' direct trust
Liu, Yang et al. [69]	Trusters' direct trust
Kamvar, Schlosser et al. [8]	Trusters' direct trust
Xiong and Liu [64]	Similarity
Golbeck2005 [21]	Trusters' direct trust
Sun, Yu et al. [37]	Recommender trust
Massa and Avesani [20]	Trusters' direct trust
Liu, Wang et al. [109]	Trusters' direct trust
Zhang and Durresi [12]	Trusters' direct trust

4.9. Social theories and machine learning combined method

4.9.1. Tang, Gao et al.

Tang, Gao et al. proposed a low rank matrix factorization method – hTrust [119] to predict trust relationships. Besides considering latent factors, it also considers homophily effect which is widely existed in online social networks. Basically, similar users are more likely to trust each other than others. Therefore, in the objective function, it includes the similarity of two users' latent vectors as one regularization term.

4.9.2. Yao, Tong et al.

Matri [24] treats trust aspects as latent factors and uses matrix factorization to predict trust values. Similar to the classic collaborative filtering algorithm, there are two matrices in Matri: truster matrix and trustee matrix. It also adapts four trust propagation operators from [50]. Besides these four operators, it also takes global bias, truster bias and trustee bias into account. It combines four social trust propagation operators with the matrix factorization method.

We can see from above that many schemes use weighted mean to aggregate trust from multiple trust paths; however, their weights are assigned differently. We summarize their weights in Table 2.

5. Attacks in trust management systems and their defense mechanisms

Security is now a very hot topic in many fields of computer science [120–122]. Trust management systems can help to mitigate the damage in many applications, such as access control, authentication, secure service provision and secure routing [46]; however, they themselves can be the targets of malicious attackers, too [123,124]. In this section, we discuss several potential attacks in trust management systems.

Attackers in trust management systems are malicious participants who are motivated either by selfish or malicious intentions [125]. Selfish attackers launch attacks for their own benefits, while malicious attackers aim to degrade others' trust and then affect the system's performance [34,126]. According to Hoffman et al. [34], attackers can be classified into insiders and outsiders. Insiders are those who can get access to the systems and participate in the systems as normal participants, while outsiders are not authorized by the systems. Obviously, attackers inside the systems can

cause more damage than outsiders. Therefore, many traditional approaches focus on authenticating participants' identities by using cryptography primitives [127,128]. In today's life, identity authentication is not sufficient. It is very easy for attackers to get into the systems in many open environment applications [34], which include online social communities. Authorized participants in online social communities may behave badly, e.g. providing misleading information. In such situations, trust is introduced for the purpose of helping participants to avoid cooperating with potential malicious attackers. In [129], Rasmussen and Jansson used hard security to refer identity authentication, and treated social control mechanisms, e.g. trust, as soft security. In this paper we only focus on soft security.

Attackers can behave in various ways for different purposes. Based on this, Hoffman et al. classified attacks in reputation systems into self-promoting, whitewashing, slandering, orchestrated and denial of service [34]. In [46], authors listed misleading feedback attack, discrimination attack, on-off attack, Sybil attack and new comer attack. There are even more types of attacks in [130]. Some of those attacks, such as self-promoting and slandering, are considered for reputation systems or global trust only. While some of them are application dependent, e.g. imbalance value attack, denial of service. In this paper, we mainly focus on potential attacks that can happen to local trust. We list four types of attacks based on attackers' behaviors. Note that we consider Sybil attack [131] as an auxiliary method for attackers to achieve their goals. So, it can be launched with any of the following attacks.

5.1. Naive attack

As pointed out by Wang et al. [46], attackers may provide misleading recommendations to their neighbors. Dishonest recommendations can affect users' decisions. Also, it can be used in reputation systems to launch the self-promoting attack and slandering attack by providing negative feedback for good participants and positive feedback for their conspirators. In the naive attack, attackers blindly provide dishonest recommendations and have no knowledge about the systems. They do not realize that their dishonest recommendations may not be considered if they are untrustworthy to other participants.

To defend against the naive attack, when considering intermediary participants' recommendations, many systems only take into account recommendations from trustworthy neighbors [12,21,31,132]. Using weighted mean, attackers' recommendations will be weighted by their own trust levels. Some schemes, such as [21] and [31], set certain thresholds to select trustworthy paths. In order for the recommendations to be considered, trust paths' trust levels must be higher than the thresholds. In such cases, if participants do not trust attackers, the dishonest recommendations have no or very little impact. There exist few other mechanisms to defend against the naive attack, e.g. clustering [46]; however, we do not consider them in this paper as we only focus on trust-based mechanisms.

5.2. Traitor attack

As we discussed, if attackers' trust levels are low, their recommendations can only have very little impact on other participants' decisions. This is intuitive and can also be learned by attackers. Therefore, it is possible that before attackers begin to disseminate dishonest recommendations, they will provide honest recommendations for a period of time in order to become trustworthy neighbors of normal participants. Such an attack is called the traitor attack (or On-off attack) in [46,133] because attackers can suddenly change their behaviors.

If we only consider a single attacker's behavior, the traitor attack cannot be completely eliminated. Before the first malicious behavior happens, attackers have good trust levels because of their previously disguised behavior. There is no way to predict attackers' first bad behavior based on their former trust levels. Therefore, when we discuss the defense to the traitor attack, we refer to defending against attackers' following consecutive bad behavior. The purpose of defense mechanisms is to detect attackers and remove them or mitigate their impact as soon as possible. One straightforward way is that bad behavior is given more weight than good behavior [133]. This means that participants have to behave good for a long time in order to become trustworthy, while their trust can decrease dramatically even if they only behave badly one time [11,64]. It requires systems to update trust in a timely manner. Under this situation, attackers' sequential dishonest recommendations will not be accepted as their trust decreases immediately after the first dishonest recommendations. Apart from this, systems can put higher weights on recent evidence than previous evidence such that trust is mainly determined by recent behavior (also called forgetting factor) [64,134]. To summarize, these strategies aim to reduce attackers' trust immediately once they behave badly.

5.3. Whitewashing attack

Attackers having very low trust levels may be interested in discarding their current identities and re-enter the systems. This is called the whitewashing attack since attackers can behave as new comers and hide their bad histories [135]. Whitewashing attack is a very common phenomenon in many online social communities because participants are able to create identities and re-enter the systems very easily [136]. Whitewashing attack is especially attractive in systems where bad history can lead to negative trust levels. For example, attackers' trust is negative because of their previous malicious behaviors. Then, they only need to re-enter the systems, and their trust becomes zero, which is better than before.

Defense mechanisms for the whitewashing attack can be divided into two aspects. First, systems can prevent participants from creating multiple identities or make it expensive. For instance, some systems require users to provide social security numbers or biometrics to register for identities. This kind of defense mechanism is related to hard security, which is beyond the scope of this paper. On the other hand, systems can assign the lowest trust levels to the new comers such that there is no incentive for participants to re-enter the systems again. In those systems which consider confidence, attackers will lose their former confidence if they re-enter the systems [12]. Of course, it is a challenge for normal new comers to become trustworthy, which is known as the cold start problem [137].

5.4. Collusion attack

Attacks mentioned previously can be launched together by either a single attacker or several attackers. We refer to the collusion attack the combination of multiple attacks, and it can be launched by a number of attackers [125,138].

In order to get identities in a system, malicious users can launch the Sybil attack first. Sybil attack is one of the most popular attacks in online systems. In the Sybil attack, a single user is able to create many identities and behave as if there were multiple participants. In some extreme cases, attackers can create millions of identities such that the system will be dominated by Sybil accounts.

Compared with the above three attacks, the collusion attack is more complicated and difficult to detect [125]. In the collusion attack, attackers can act in several different ways to achieve their

goals. In addition, attackers can divide malicious identities into different groups, and each group has their own responsibility at a given time. For example, in reputation systems, one group of accounts rate their conspirators with high trust in order to increase their global trust. Their conspirators are responsible for disseminating dishonest recommendations. There can be many other tasks divided among groups. To make it more complicated, attackers can switch their roles during the process [125].

As the collusion attack is the combination of different types of attacks, defense mechanisms also need to employ several methods together. There are some works trying to find out colluded attackers. In [133], Sun et al. developed a defense mechanism with temporal and correlation analysis. In order to find approaches to defend against the collusion attack, it first analyzes one type of the collusion attack, which they called RepTrap attack. In RepTrap attack, attackers have several features and behavior patterns. TAUCA, which is the defense mechanism, has three components: change detection, user correlation calculation and malicious user group identification. Change detector is used to monitor the changing trend of behavior (rating). Then TAUCA analyzes the correlation among suspicious participants. Finally TAUCA can identify malicious participants' groups. More details about TAUCA can be found in [133]. Colluded attackers can be considered as clusters in graph models as they are similar to each other. With this observation, clustering algorithms are used to find out groups of participants in the systems.

From what we discussed above, behavior of the collusion attack can be changed with different attackers' strategies. Although we have seen examples of defense mechanisms to defend against the collusion attack, we should note that they all have certain assumptions about attackers' behavior. For example, in order to develop defense mechanisms, they need to know attackers' behavior patterns in advance, which is a tough task in reality.

To summarize, we can see that attackers have many methods to damage the systems. For example, attackers can launch the Sybil attack and the naive attack together. Although we discussed some defense mechanisms to deal with such attacks, there is a great need for further research work in this field. More importantly, in many applications, the defensive strategies should be used together in order to defend effectively against attackers. Finally, remember that attackers can also learn defense mechanisms and become immune to them. Therefore, it is like an "Arms race" between attackers and defense mechanisms.

6. Analysis of vulnerability to attacks

In the above section, we listed four types of potential attacks in trust management systems. As the collusion attack is dependent on attackers' strategies which are different in applications, in this section, we analyze existing schemes' vulnerabilities to the naive attack, the traitor attack and the whitewashing attack. We examine existing schemes to see whether they have the defense mechanisms we mentioned in Section 5 to defend against corresponding attacks. For those systems which do not consider trust propagation, such as [11], we do not analyze their vulnerabilities to attacks. Also, for machine learning based methods, we do not analyze their vulnerabilities.

Abdul-Rahman and Hailes in [43] proposed a trust management system which is used in virtual communities. Their model propagates and aggregates trust by weighted mean, where weights are intermediary participants' recommender trust. Therefore, it is robust to the naive attack as naive attackers' dishonest recommendations will be discounted. Also, the truster updates recommender trust after each recommendation finishes. In such situations, if attackers suddenly change their behavior, their recommender trust will be decreased immediately. So it can defend against the traitor attack as well. But it is vulnerable to the whitewashing attack as new comers have neutral trust levels, which is better than a bad trust level, e.g. "very untrustworthy".

Subjective logic [70] proposed by Jøsang defines trust following belief theory. In this scheme, new comers have the lowest trust, therefore, the whitewashing attack does not have any impact. In trust transitivity, as evidence is discounted by intermediary participants' trust, it is robust to the naive attack. Unlike [43], Subjective Logic does not compare recommendations with the truster's own experiences. Also, it does not take into account temporal information and forgetting factor, so it is vulnerable to the traitor attack. CertainTrust [71], which is built based on Subjective Logic, has the same characters as Subjective Logic, as well as [69] and [106].

Kamvar et al. [8] uses normalized local trust for each participant. New comers have the lowest trust levels, therefore, there is no incentive for attackers to re-enter the system. It uses weighted mean mechanism to defend against the naive attack. Unfortunately, [8] does not contain any defense mechanism for the traitor attack. Hence it is vulnerable to the traitor attack.

Xiong and Liu proposed PeerTrust [64] for P2P networks. It takes many factors into account in modeling trust, including time decaying, different weights for positive and negative evidence, which makes it robust to the traitor attack. Naive attackers' recommendations are discounted by their trust, so it is robust to the naive attack as well. There is no incentive for attackers to re-enter the system. Those features, combined together, make PeerTrust more robust to the collusion attack compared with other schemes.

TidalTrust [21] is robust to the naive attack as it uses weighted mean for trust aggregation. Also, the whitewashing attack is avoided because new comers have the lowest trust levels; however it does not contain any defense mechanisms for the traitor attack.

Sun, Yu et al. used a probability based trust in [37]. They put penalties on bad behavior by dramatically decreasing trust. Also, trust can only increase gradually even though participants behave very good. Therefore, it is robust to the traitor attack. As it uses weighted mean for trust transitivity and aggregation, it is robust to the naive attack. It is vulnerable to the whitewashing attack as new comers have better trust levels than bad participants (negative levels).

In MoleTrust [20], Massa used one continuous value to represent trust. Because only trustworthy paths will be accepted in his model, it is robust to the naive attack. It is also robust to the whitewashing attack as new comers have the lowest trust. But it is vulnerable to the traitor attack.

Liu et al. [109] use weighted mean as well, so it is robust to the naive attack. Although it takes recommendation roles into account, it does not update them after each recommendation. Therefore, it is vulnerable to the traitor attack. Because new comers have the lowest trust levels, it is robust to the whitewashing attack.

In [12], trust evaluation is considered as a "measurement". Trust is defined by rating values between participants and confidence is related to the number of ratings. Both of them are continuous values between 0 and 1. Their model is robust to the naive attack and the whitewashing attack as it uses weighted mean and assigns the lowest trust levels for new comers.

In [51], Golbeck proposed a scheme to infer binary trust in social networks. When considering recommendations, only trustworthy neighbors' recommendations are selected. Therefore, it is robust to the naive attack. It is also robust to the whitewashing attack as new comers are not trustworthy in the beginning; however it is vulnerable to the traitor attack.

Guha [50] used four atomic operators to calculate trust and distrust matrices. In his model, both trust and distrust can be propagated. As he used distrust, the whitewashing attack is possible in his model. Trust is discounted when it propagates through the chains, so it is robust to the naive attack. Unfortunately, it is

Table 3
Vulnerability to attacks.

Schemes	Naive attack	Traitor attack	Whitewashing attack
Abdul-Rahman, Hailes et al. [43]	Weighted mean	Updating recommender trust	No
Jøsang [70]	Weighted mean	No	Lowest trust level for new comer
Sabestian [71]	Weighted mean	No	Lowest trust level for new comer
Wang and Singh [67]	Weighted mean	No	Lowest trust level for new comer
Liu, Yang et al. [69]	Weighted mean	No	Lowest trust level for new comer
Kamvar, Schlosser et al. [8]	Weighted mean	No	Lowest trust level for new comer
Xiong and Liu [64]	Weighted mean	Forgetting factor, time window	Lowest trust level for new comer
Golbeck2005 [21]	Weighted mean	No	Lowest trust level for new comer
Sun, Yu et al. [37]	Weighted mean	Forgetting factor	No
Massa and Avesani [20]	Weighted mean	No	Lowest trust level for new comer
Liu, Wang et al. [80]	Weighted mean	No	Lowest trust level for new comer
Zhang and Durresi [12]	Weighted mean	No	Lowest trust level for new comer
Golbeck2006 [51]	Threshold	No	Lowest trust level for new comer
Guha and Kumar [50]	Weighted mean	No	No
Zhang and Mao [53]	Weighted mean	No	No
Victor, Cornelis et al. [60]	Threshold	No	No
Verbiest, Cornelis et al. [111]	Threshold	No	No
Wang and Wu [68]	Weights adjusted by Bayesian network	No	Lowest trust level for new comer
Huang, Kimmig et al. [113]	No	No	Dependent on applications
Zhan and Li [112]	Most trustworthy path	No	Lowest trust level for new comer
Hao, Min et al. [103]	Most trustworthy path	No	Lowest trust level for new comer

vulnerable to the traitor attack. Zhang and Mao [53] adopts Guha's work [50] and changes four atomic operators to two. But they have the same characters regarding attacks.

Victor used bi-lattice based trust in [60]. Knowledge defect captures to what extent participants are certain about their estimations. It is vulnerable to the whitewashing attack as new comers have better trust levels than bad participants. As it considers thresholds in trust transitivity, it is robust to the naive attack. It is vulnerable to the traitor attack as there is no defense mechanisms. Verbiest et al. [111] has the same properties.

Wang and Wu [68] evaluate trust similar to [70], therefore, it is robust to the whitewashing attack. It uses the parameterized family of Frank t-norm to combine trust paths, where discounting rates are controlled by participants. So it provides opportunity to defend against the naive attack. It does not update the discounting rate, hence it is vulnerable to the traitor attack.

Huang et al. [113] propagate and aggregates trust following balance theory and status theory. In this cases, the inferred trust is determined by the corresponding triangles. Therefore, it is vulnerable to the naive attack and the traitor attack. It is unclear for the whitewashing attack as the lowest trust value is dependent on specific applications.

Zhao et al. [112] and Hao et al. [103] only select the most trustworthy paths to aggregate trust paths. Therefore, they are robust to the naive attack. Also, as the new comer has the lowest trust degree, both of them are robust to the whitewashing attack.

We summarize the above analyzed results in Table 3. For each type of attack, if the scheme is robust to the attack, we list which mechanism is used accordingly. For those schemes which are vulnerable to the attacks, we represent it by "No" in the corresponding attacks. We can see that although the naive attack is considered in many schemes, only few schemes take the traitor attack into account.

7. Conclusions

In this paper, we discuss the urgent need of trust management systems in many online social communities. We investigate how trust is defined by researchers from different disciplines and how can it be represented in the field of computer science. As we can see, it has various computational models depending on how people understand it. The definitions and representations of trust are basics for trust management systems. Besides trust, confidence is another important concept in trust-based systems.

Furthermore, we present different trust management schemes. Many of them have two important operators: transitivity and aggregation operators. This can largely increase the number of connected participants. Aggregation operator, which always works together with transitivity operator, deals with the situation when there are more than one parallel trust path between the truster and the trustee.

Finally, we review some potential trust attacks in trust management systems. We describe four types of behaviors in these attacks. We analyze existing schemes' vulnerabilities to the attacks. If they are robust to the attacks, we list which defense mechanisms they use.

Compared with previous survey papers in this field, we provided a comprehensive survey that takes two challenges – trust modeling and trust inference, into account. In addition to that, we also discussed four types of potential attacks that can happen in trust management systems.

8. Competing interests

The authors declare that they have no competing interests.

9. Author's contributions

Yefeng Ruan reviewed the literature work and drafted the paper. Arjan Durresi proofread the draft and provided comments and suggestions to improve the draft. Yefeng Ruan was also in charge of submitting the paper and corresponding with the editors of the journal. All authors read and approved the final manuscript.

Acknowledgment

This work is partially supported by National Science Foundation under Grant No. 1547411.

References

[1] B.A. Huberman, D.M. Romero, F. Wu, Social networks that matter: Twitter under the microscope, Available at SSRN 1313405 (2008).
[2] Q. Shambour, J. Lu, A hybrid trust-enhanced collaborative filtering recommendation approach for personalized government-to-business e-services, Int. J. Intell. Syst. 26 (9) (2011) 814–843.
[3] Q. Shambour, J. Lu, A trust-semantic fusion-based recommendation approach for e-business applications, Decis. Support Syst. 54 (1) (2012) 768–780.
[4] H. Fang, J. Zhang, M. Şensoy, N. Magnenat-Thalmann, Reputation mechanism for e-commerce in virtual reality environments, Electron. Commerce Res. Appl. 13 (6) (2014) 409–422.
[5] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2) (2007) 618–644.

[6] P. Massa, P. Avesani, Controversial users demand local trust metrics: an experimental study on epinions.com community, in: Proceedings of the 20th National Conference on Artificial Intelligence - Volume 1, in: AAAI'05, AAAI Press, 2005, pp. 121–126.

[7] P. Massa, P. Avesani, Trust-aware recommender systems, in: Proceedings of the 2007 ACM Conference on Recommender Systems, ACM, 2007, pp. 17–24.

[8] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina, The eigentrust algorithm for reputation management in p2p networks, in: Proceedings of the 12th International Conference on World Wide Web, ACM, 2003, pp. 640–651.

[9] X. Li, F. Zhou, X. Yang, Scalable feedback aggregating (sfa) overlay for large-scale p2p trust management, Parallel Distrib. Syst., IEEE Trans. 23 (10) (2012) 1944–1957.

[10] M. Tavakolifard, On some challenges for online trust and reputation systems Ph.D. thesis, NTNU Trykk, 2012.

[11] M. Stephen, Formalising trust as a computational concept Ph.D. thesis, University of Stirling, scotland, 1994.

[12] P. Zhang, A. Durresi, Trust management framework for social networks, in: Proceedings of the IEEE International Conference on Communications, 2012, pp. 1042–1047.

[13] W. Sherchan, S. Nepal, C. Paris, A survey of trust in social networks, ACM Comput. Surveys (CSUR) 45 (4) (2013) 47.

[14] J. Golbeck, Trust on the world wide web: a survey, Foundations Trends in Web Sci. 1 (2) (2006) 131–197.

[15] K. Chen, G. Liu, H. Shen, F. Qi, Sociallink: utilizing social network and transaction links for effective trust management in p2p file sharing systems, in: Peer-to-Peer Computing (P2P), 2015 IEEE International Conference on, 2015, pp. 1–10, doi:10.1109/P2P.2015.7328527.

[16] S. Sedhain, S. Sanner, D. Braziunas, L. Xie, J. Christensen, Social collaborative filtering for cold-start recommendations, in: Proceedings of the 8th ACM Conference on Recommender systems, ACM, 2014, pp. 345–348.

[17] G. Guo, J. Zhang, D. Thalmann, Merging trust in collaborative filtering to alleviate data sparsity and cold start, Knowl.-Based Syst. 57 (2014) 57–68.

[18] E. Dumbill, XML Watch: finding friends with XML and RDF, Technical Report, IBM Developers Works, 2002.

[19] A. Jøsang, E. Gray, M. Kinateder, Analysing topologies of transitive trust, in: Proceedings of the First International Workshop on Formal Aspects in Security & Trust (FAST2003), Pisa, Italy, 2003, pp. 9–22.

[20] P. Massa, P. Avesani, Trust metrics on controversial users: balancing between tyranny of the majority, Int. J. Semantic Web Inform. Syst. (IJSWIS) 3 (1) (2007) 39–64.

[21] J.A. Golbeck, Computing and applying trust in web-based social networks Ph.D. thesis, University of Maryland at College Park, College Park, MD, USA Ph.D. thesis, 2005. AAI3178583.

[22] U. Kuter, J. Golbeck, Sunny: a new algorithm for trust inference in social networks using probabilistic confidence models, in: Proceedings of the 22nd National Conference on Artificial Intelligence - Volume 2, in: AAAI'07, AAAI Press, 2007, pp. 1377–1382.

[23] Y. Wang, C.-W. Hang, M.P. Singh, A probabilistic approach for maintaining trust based on evidence, J. Artif. Int. Res. 40 (1) (2011) 221–267.

[24] Y. Yao, H. Tong, X. Yan, F. Xu, J. Lu, Matri: a multi-aspect and transitive trust inference model, in: Proceedings of the 22Nd International Conference on World Wide Web, in: WWW '13, International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 2013, pp. 1467–1476.

[25] Y. Yao, H. Tong, F. Xu, J. Lu, Subgraph extraction for trust inference in social networks, in: Encyclopedia of Social Network Analysis and Mining, Springer, 2014, pp. 2084–2098.

[26] D. O'Doherty, S. Jouili, P. Van Roy, Towards trust inference from bipartite social networks, in: Proceedings of the 2Nd ACM SIGMOD Workshop on Databases and Social Networks, in: DBSocial '12, ACM, New York, NY, USA, 2012, pp. 13–18, doi:10.1145/2304536.2304539.

[27] H. Fang, G. Guo, J. Zhang, Multi-faceted trust and distrust prediction for recommender systems, Decis. Support Syst. 71 (2015) 37–47.

[28] A. Shabut, K. Dahal, S. Bista, I. Awan, Recommendation based trust model with an effective defence scheme for manets, Mobile Comput. IEEE Trans. 14 (10) (2015) 2101–2115, doi:10.1109/TMC.2014.2374154.

[29] J. Sabater, C. Sierra, Review on computational trust and reputation models, Artif. Intell. Rev. 24 (1) (2005) 33–60.

[30] S. Grabner-Kräuter, E.A. Kaluscha, Empirical research in on-line trust: a review and critical assessment, Int. J. Human-Comput. Stud. 58 (6) (2003) 783–812.

[31] S. Ries, J. Kangasharju, M. Mühlhäuser, A classification of trust systems, in: Proceedings of the 2006 International Conference on on the Move to Meaningful Internet Systems: AWeSOMe, CAMS, COMINF, IS, KSinBIT, MIOS-CIAO, MONET - Volume Part I, in: OTM'06, Springer-Verlag, Berlin, Heidelberg, 2006, pp. 894–903, doi:10.1007/11915034_114.

[32] S. Ruohomaa, L. Kutvonen, Trust management survey, in: Proceedings of the Third International Conference on Trust Management, in: iTrust'05, Springer-Verlag, Berlin, Heidelberg, 2005, pp. 77–92, doi:10.1007/11429760_6.

[33] S. Spitz, Y. Tüchelmann, A survey of security issues in trust and reputation systems for e-commerce, in: Autonomic and Trusted Computing, Springer, 2011, pp. 203–214.

[34] K. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Comput. Surv. 42 (1) (2009) 1:1–1:31, doi:10.1145/1592451.1592452.

[35] B.W. Husted, The ethical limits of trust in business relations, Bus. Ethics Quart. (1998) 233–248.

[36] J.-H. Cho, K. Chan, S. Adali, A survey on trust modeling, ACM Comput. Surv. 48 (2) (2015) 28:1–28:40, doi:10.1145/2815595.

[37] Y. Sun, W. Yu, Z. Han, K. Liu, Trust modeling and evaluation in ad hoc networks, in: Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE, 3, 2005, p. 6, doi:10.1109/GLOCOM.2005.1577971.

[38] S. Che, R. Feng, X. Liang, X. Wang, A lightweight trust management based on bayesian and entropy for wireless sensor networks, Security Commun. Netw. 8 (2) (2015) 168–175, doi:10.1002/sec.969.

[39] C.-N. Ziegler, J. Golbeck, Investigating interactions of trust and interest similarity, Decis. Support Syst. 43 (2) (2007) 460–475, doi:10.1016/j.dss.2006.11.003.

[40] N. Yang, A similarity based trust and reputation management framework for vanets, Int. J. Future Gen. Commun. Netw. 6 (2) (2013) 25–34.

[41] C. Fernandez-Gago, I. Agudo, J. Lopez, Building trust from context similarity measures, Comput. Standards Interfaces 36 (4) (2014) 792–800. http://dx.doi.org/10.1016/j.csi.2013.12.012. Security in Information Systems: Advances and new Challenges.

[42] D.H. McKnight, N.L. Chervany, The meanings of trust, Technical Report, University of Minnesota, 1996.

[43] A. Abdul-Rahman, S. Hailes, Supporting trust in virtual communities, in: System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on, 2000, p. 9 vol.1, doi:10.1109/HICSS.2000.926814.

[44] P. Massa, A survey of trust use and modeling in real online systems, Trust E-services (2007) 51–83.

[45] J.-H. Cho, A. Swami, I.-R. Chen, A survey on trust management for mobile ad hoc networks, Commun. Surveys Tutorials, IEEE 13 (4) (2011) 562–583, doi:10.1109/SURV.2011.092110.00088.

[46] D. Wang, T. Muller, Y. Liu, J. Zhang, Towards robust and effective trust management for security: a survey, in: Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on, 2014, pp. 511–518, doi:10.1109/TrustCom.2014.65.

[47] C. Ding, C. Yueguo, C. Weiwei, A Survey Study on Trust Management in p2p Systems, Department of Computer Science, School of Computing-National University of Singapore, 2004.

[48] H. Ma, Z. Hu, Cloud service recommendation based on trust measurement using ternary interval numbers, in: Smart Computing (SMARTCOMP), 2014 International Conference on, 2014, pp. 21–24, doi:10.1109/SMARTCOMP.2014.7043834.

[49] H. Shakeri, A. Ghaemi Bafghi, A layer model of a confidence-aware trust management system, Int. J. Inform. Sci. Intell. Syst. 3 (1) (2014) 73–90.

[50] R. Guha, R. Kumar, P. Raghavan, A. Tomkins, Propagation of trust and distrust, in: Proceedings of the 13th international conference on World Wide Web, in: WWW '04, ACM, New York, NY, USA, 2004, pp. 403–412, doi:10.1145/988672.988727.

[51] J. Golbeck, J. Hendler, Inferring binary trust relationships in web-based social networks, ACM Trans. Internet Technol. (TOIT) 6 (4) (2006) 497–529.

[52] J. Leskovec, D. Huttenlocher, J. Kleinberg, Predicting positive and negative links in online social networks, in: Proceedings of the 19th International Conference on World wide web, in: WWW '10, ACM, New York, NY, USA, 2010, pp. 641–650, doi:10.1145/1772690.1772756.

[53] R. Zhang, Y. Mao, Trust prediction via belief propagation, ACM Trans. Inform. Syst. (TOIS) 32 (3) (2014) 15.

[54] P. Massa, P. Avesani, Trust-aware collaborative filtering for recommender systems, On Move Meaningful Internet Syst. 2004 3290 (2004).

[55] Y.L. Sun, W. Yu, Z. Han, K. Liu, Information theoretic framework of trust modeling and evaluation for ad hoc networks, Selected Areas in Commun., IEEE J. 24 (2) (2006) 305–317.

[56] M.G. Uddin, M. Zulkernine, S.I. Ahamed, Cat: a context-aware trust model for open and dynamic systems, in: Proceedings of the 2008 ACM Symposium on Applied Computing, in: SAC '08, ACM, New York, NY, USA, 2008, pp. 2024–2029, doi:10.1145/1363686.1364176.

[57] J. Zhan, X. Fang, A novel trust computing system for social networks, in: Privacy, Security, Risk and Trust (passat), 2011 Ieee Third International Conference on and 2011 Ieee Third International Conference on Social Computing (Socialcom), 2011, pp. 1284–1289, doi:10.1109/PASSAT/SocialCom.2011.236.

[58] J. Hiltunen, J. Kuusijarvi, Trust metrics based on a trusted network element, in: Trustcom/BigDataSE/ISPA, 2015 IEEE, 1, 2015, pp. 660–667, doi:10.1109/Trustcom.2015.432.

[59] L. Guo, C. Zhang, Y. Fang, A trust-based privacy-preserving friend recommendation scheme for online social networks, Depend. Secure Comput. IEEE Trans. 12 (4) (2015) 413–427, doi:10.1109/TDSC.2014.2355824.

[60] P. Victor, C. Cornelis, M.D. Cock, Trust Networks for Recommender Systems, 1st, Atlantis Publishing Corporation, 2011.

[61] S. Marsh, M.R. Dibben, Trust, untrust, distrust and mistrust–an exploration of the dark (er) side, in: Trust Management, Springer, 2005, pp. 17–33.

[62] H. Fang, J. Zhang, N.M. Thalmann, A trust model stemmed from the diffusion theory for opinion evaluation, in: Proceedings of the 2013 International Conference on Autonomous Agents and Multi-agent Systems, in: AAMAS '13, International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 2013, pp. 805–812.

[63] S. Nepal, W. Sherchan, C. Paris, Strust: a trust model for social networks, in: Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on, 2011, pp. 841–846, doi:10.1109/TrustCom.2011.112.

[64] L. Xiong, L. Liu, Peertrust: supporting reputation-based trust for peer-to-peer electronic communities, Knowl. Data Eng., IEEE Trans. 16 (7) (2004) 843–857.
[65] H. Zhang, Y. Wang, X. Zhang, E.-P. Lim, Reputationpro: the efficient approaches to contextual transaction trust computation in e-commerce environments, ACM Trans. Web 9 (1) (2015) 2:1–2:49, doi:10.1145/2697390.
[66] X. Zheng, Y. Wang, M.A. Orgun, G. Liu, H. Zhang, Social context-aware trust prediction in social networks, in: Service-Oriented Computing, Springer, 2014, pp. 527–534.
[67] Y. Wang, M.P. Singh, Formal trust model for multiagent systems, in: Proceedings of the 20th International Joint Conference on Artifical Intelligence, in: IJCAI'07, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2007, pp. 1551–1556.
[68] G. Wang, J. Wu, Multi-dimensional evidence-based trust management with multi-trusted paths, Future Gen. Comput. Syst. 27 (5) (2011) 529–538.
[69] G. Liu, Q. Yang, H. Wang, X. Lin, M.P. Wittie, Assessment of multi-hop interpersonal trust in social networks by three-valued subjective logic, in: INFOCOM, 2014 Proceedings IEEE, IEEE, 2014, pp. 1698–1706.
[70] A. Jøsang, A logic for uncertain probabilities, Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 9 (3) (2001) 279–311.
[71] S. Ries, Certain trust: A trust model for users and agents, in: Proceedings of the 2007 ACM Symposium on Applied Computing, in: SAC '07, ACM, New York, NY, USA, 2007, pp. 1599–1604, doi:10.1145/1244002.1244342.
[72] T. DuBois, J. Golbeck, A. Srinivasan, Predicting trust and distrust in social networks, in: Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on, 2011, pp. 418–424, doi:10.1109/PASSAT/SocialCom.2011.56.
[73] Y. Ruan, L. Alfantoukh, A. Fang, A. Durresi, Exploring trust propagation behaviors in online communities, in: Network-Based Information Systems (NBiS), 2014 17th International Conference on, 2014, pp. 361–367, doi:10.1109/NBiS.2014.91.
[74] Y. Ruan, L. Alfantoukh, A. Durresi, Exploring stock market using twitter trust network, in: Advanced Information Networking and Applications (AINA), 2015 IEEE 29th International Conference on, 2015, pp. 428–433, doi:10.1109/AINA.2015.217.
[75] S. Adali, R. Escriva, M.K. Goldberg, M. Hayvanovych, M. Magdon-Ismail, B.K. Szymanski, W.A. Wallace, G. Williams, Measuring behavioral trust in social networks, in: Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on, IEEE, 2010, pp. 150–152.
[76] H.J. Ahn, A new similarity measure for collaborative filtering to alleviate the new user cold-starting problem, Inf. Sci. 178 (1) (2008) 37–51, doi:10.1016/j.ins.2007.07.024.
[77] T. Bhuiyan, Trust for Intelligent Recommendation, Springer, 2013.
[78] I.-R. Chen, J. Guo, F. Bao, Trust management for soa-based iot and its application to service composition, Services Comput., IEEE Trans. PP (99) (2014), doi:10.1109/TSC.2014.2365797. 1–1
[79] J. Golbeck, Trust and nuanced profile similarity in online social networks, ACM Trans. Web 3 (4) (2009) 12:1–12:33, doi:10.1145/1594173.1594174.
[80] G. Liu, Y. Wang, M.A. Orgun, et al., Trust transitivity in complex social networks, in: AAAI, 11, 2011, pp. 1222–1229.
[81] D. Gambetta, Can we trust trust? in: Trust: Making and Breaking Cooperative Relations, Basil Blackwell, 1988, pp. 213–237.
[82] A. Jsang, R. Ismail, The beta reputation system, in: Proceedings of the 15th Bled Electronic Commerce Conference, 5, 2002, pp. 2502–2511.
[83] S. Knapskog, A metric for trusted systems, in: Proceedings of the 21st National Security Conference, Citeseer, 1998, pp. 16–29.
[84] M. Tavakolifard, K.C. Almeroth, J.A. Gulla, Does social contact matter? Modelling the hidden web of trust underlying twitter, Proceedings of the 22Nd International Conference on World Wide Web, WWW '13 Companion, ACM, New York, NY, USA, 2013, pp. 981–988, doi:10.1145/2487788.2488095.
[85] D. Goldberg, D. Nichols, B.M. Oki, D. Terry, Using collaborative filtering to weave an information tapestry, Commun. ACM 35 (12) (1992) 61–70, doi:10.1145/138859.138867.
[86] S. Tadelis, The economics of reputation and feedback systems in e-commerce marketplaces, Internet Comput., IEEE 20 (1) (2016) 12–19, doi:10.1109/MIC.2015.140.
[87] R. Zhou, K. Hwang, Powertrust: a robust and scalable reputation system for trusted peer-to-peer computing, Parallel Distrib. Syst. IEEE Trans. 18 (4) (2007) 460–473, doi:10.1109/TPDS.2007.1021.
[88] T. Yajima, A. Matsumoto, H. Shigeno, Ptrust: Provisional value based trust for reputation aggregation in peer-to-peer networks, in: Access Spaces (ISAS), 2011 1st International Symposium on, 2011, pp. 180–185, doi:10.1109/ISAS.2011.5960944.
[89] W. Xue, Y. Liu, K. Li, Z. Chi, G. Min, W. Qu, Dhtrust: a robust and distributed reputation system for trusted peer-to-peer networks, Concurrency Comput 24 (10) (2012) 1037–1051, doi:10.1002/cpe.1749.
[90] X. Fan, M. Li, J. Ma, Y. Ren, H. Zhao, Z. Su, Behavior-based reputation management in p2p file-sharing networks, J. Comput. Syst. Sci. 78 (6) (2012) 1737–1750.
[91] Z. Shen, N. Sundaresan, Reprank: reputation in a peer-to-peer online system, in: Proceedings of the 22Nd International Conference on World Wide Web, in: WWW '13 Companion, ACM, New York, NY, USA, 2013, pp. 163–164, doi:10.1145/2487788.2487868.
[92] Z. Yan, Y. Chen, Y. Shen, Percontrep: a practical reputation system for pervasive content services, J. Supercomput. 70 (3) (2014) 1051–1074.
[93] H. Rahimi, H.E. Bakkali, Ciosos: combined idiomatic-ontology based sentiment orientation system for trust reputation in e-commerce, in: International Joint Conference, Springer, 2015, pp. 189–200.
[94] K. Chen, H. Shen, K. Sapra, G. Liu, A social network based reputation system for cooperative p2p file sharing, Parallel Distrib. Syst. IEEE Trans. 26 (8) (2015) 2140–2153, doi:10.1109/TPDS.2014.2346192.
[95] C. Wu, T. Luo, F. Wu, G. Chen, An endorsement-based reputation system for trustworthy crowdsourcing, in: Computer Communications Workshops (INFOCOM WKSHPS), 2015 IEEE Conference on, 2015, pp. 89–90, doi:10.1109/INFCOMW.2015.7179357.
[96] L. Guo, C. Zhang, Y. Fang, P. Lin, A privacy-preserving attribute-based reputation system in online social networks, J. Comput. Sci. Technol. 30 (3) (2015) 578–597, doi:10.1007/s11390-015-1547-9.
[97] I. Perfilieva, J. Močkoř, Mathematical principles of fuzzy logic, Springer Science & Business Media, 1999.
[98] R. Falcone, G. Pezzulo, C. Castelfranchi, A fuzzy approach to a belief-based trust computation, in: Trust, reputation, and security: theories and practice, Springer, 2003, pp. 73–86.
[99] V. Kant, K.K. Bharadwaj, Fuzzy computational models of trust and distrust for enhanced recommendations, Int. J. Intell. Syst. 28 (4) (2013) 332–365, doi:10.1002/int.21579.
[100] K. Nafi, T. Kar, M. Hossain, M. Hashem, A fuzzy logic based certain trust model for e-commerce, in: Informatics, Electronics Vision (ICIEV), 2013 International Conference on, 2013, pp. 1–6, doi:10.1109/ICIEV.2013.6572693.
[101] A. Aref, T. Tran, Using fuzzy logic and q-learning for trust modeling in multiagent systems, in: Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on, 2014, pp. 59–66, doi:10.15439/2014F482.
[102] X. Liu, A. Datta, E.-P. Lim, Computational Trust Models and Machine Learning, CRC Press, 2014.
[103] F. Hao, G. Min, M. Lin, C. Luo, L. Yang, Mobifuzzytrust: An efficient fuzzy trust inference mechanism in mobile social networks, Parallel Distrib. Syst., IEEE Trans. 25 (11) (2014) 2944–2955, doi:10.1109/TPDS.2013.309.
[104] A. Jøsang, G. Guo, M.S. Pini, F. Santini, Y. Xu, Combining recommender and reputation systems to produce better online advice, in: Modeling Decisions for Artificial Intelligence, Springer, 2013, pp. 126–138.
[105] S.D. Ramchurn, N.R. Jennings, et al., A computational trust model for multi-agent interactions based on confidence and reputation, in: Proceedings of 6th International Workshop of Deception, Fraud and Trust in Agent Societies, 2003, pp. 69–75.
[106] Y. Wang, M.P. Singh, Trust representation and aggregation in a distributed agent system, in: Proceedings of the 21st National conference on Artificial intelligence - Volume 2, in: AAAI'06, AAAI Press, 2006, pp. 1425–1430.
[107] A. Jøsang, T. Ažderska, S. Marsh, Trust transitivity and conditional belief reasoning, in: Trust Management VI, Springer, 2012, pp. 68–83.
[108] C.-W. Hang, Y. Wang, M.P. Singh, Operators for propagating trust and their evaluation in social networks, in: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems - Volume 2, in: AAMAS '09, International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 2009, pp. 1025–1032.
[109] G. Liu, Y. Wang, M. Orgun, Trust inference in complex trust-oriented social networks, in: Computational Science and Engineering, 2009. CSE'09. International Conference on, 4, IEEE, 2009, pp. 996–1001.
[110] E.P. Klement, R. Mesiar, E. Pap, Triangular norms, 8, Springer Science & Business Media, 2013.
[111] N. Verbiest, C. Cornelis, P. Victor, E. Herrera-Viedma, Trust and distrust aggregation enhanced with path length incorporation, Fuzzy Sets Syst. 202 (2012) 61–74. Theme: Aggregation Functions http://dx.doi.org/10.1016/j.fss.2012.02.007
[112] H. Zhao, X. Li, Vectortrust: trust vector aggregation scheme for trust management in peer-to-peer networks, J. Supercomput. 64 (3) (2013) 805–829.
[113] B. Huang, A. Kimmig, L. Getoor, J. Golbeck, A flexible framework for probabilistic models of social trust, in: Social Computing, Behavioral-Cultural Modeling and Prediction, Springer, 2013, pp. 265–273.
[114] M. Brocheler, L. Mihalkova, L. Getoor, Probabilistic similarity logic, arXiv preprint arXiv:1203.3469 (2012).
[115] P. Agrawal, V.K. Garg, R. Narayanam, Link label prediction in signed social networks, in: Proceedings of the Twenty-Third international joint conference on Artificial Intelligence, AAAI Press, 2013, pp. 2591–2597.
[116] J. Ye, H. Cheng, Z. Zhu, M. Chen, Predicting positive and negative links in signed social networks by transfer learning, in: Proceedings of the 22nd international conference on World Wide Web, International World Wide Web Conferences Steering Committee, 2013, pp. 1477–1488.
[117] J. Tang, S. Chang, C. Aggarwal, H. Liu, Negative link prediction in social media, arXiv preprint arXiv:1412.2723 (2014).
[118] Y.A. Kim, H.S. Song, Strategies for predicting local trust based on trust propagation in social networks, Knowl. Based Syst. 24 (8) (2011) 1360–1371.
[119] J. Tang, H. Gao, X. Hu, H. Liu, Exploiting homophily effect for trust prediction, in: Proceedings of the Sixth ACM International Conference on Web Search and Data Mining, in: WSDM '13, ACM, New York, NY, USA, 2013, pp. 53–62, doi:10.1145/2433396.2433405.
[120] R. Von Solms, J. Van Niekerk, From information security to cyber security, Computers Security 38 (2013) 97–102.
[121] N. Paulauskas, E. Garsva, Computer system attack classification, Elektronika ir Elektrotechnika 66 (2) (2015) 84–87.

[122] D. Basin, C. Cremers, K. Miyazaki, S. Radomirovic, D. Watanabe, Improving the security of cryptographic protocol standards, IEEE Security Privacy 13 (3) (2015) 24–31.
[123] R. Kerr, R. Cohen, Smart cheaters do prosper: defeating trust and reputation systems, in: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 2, International Foundation for Autonomous Agents and Multiagent Systems, 2009, pp. 993–1000.
[124] O.A. Wahab, J. Bentahar, H. Otrok, A. Mourad, A survey on trust and reputation models for web services: single, composite, and communities, Dec. Support Syst. 74 (2015) 121–134.
[125] Y. Sun, Z. Han, K. Liu, Defense of trust management vulnerabilities in distributed networks, Commun. Mag. IEEE 46 (2) (2008) 112–119.
[126] A.A. Irissappane, S. Jiang, J. Zhang, Towards a comprehensive testbed to evaluate the robustness of reputation systems against unfair rating attack, in: UMAP Workshops, 12, 2012.
[127] B.C. Neuman, T. Ts'o, Kerberos: an authentication service for computer networks, Commun. Mag. IEEE 32 (9) (1994) 33–38.
[128] I. Polakis, P. Ilia, F. Maggi, M. Lancini, G. Kontaxis, S. Zanero, S. Ioannidis, A.D. Keromytis, Faces in the distorting mirror: revisiting photo-based social authentication, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2014, pp. 501–512.
[129] L. Rasmusson, S. Jansson, Simulated social control for secure internet commerce, in: Proceedings of the 1996 workshop on New security paradigms, in: NSPW '96, ACM, New York, NY, USA, 1996, pp. 18–25, doi:10.1145/304851.304857.
[130] A. Jøsang, Robustness of trust and reputation systems: does it matter? in: Trust Management VI, Springer, 2012, pp. 253–262.
[131] J.R. Douceur, The sybil attack, in: Peer-to-peer Systems, Springer, 2002, pp. 251–260.
[132] H. Tosun, J.W. Sheppard, Incorporating evidence into trust propagation models using markov random fields, in: Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on, 2011, pp. 263–269, doi:10.1109/PERCOMW.2011.5766880.
[133] Y. Sun, Y. Liu, Security of online reputation systems: the evolution of attacks and defenses, Signal Process. Mag. IEEE 29 (2) (2012) 87–97, doi:10.1109/MSP.2011.942344.
[134] Y.L. Sun, Z. Han, W. Yu, K.R. Liu, A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks., in: INFOCOM, 2006, 2006, pp. 1–13.
[135] K. Lai, M. Feldman, I. Stoica, J. Chuang, Incentives for cooperation in peer–to-peer networks, in: Workshop on economics of peer-to-peer systems, 2003, pp. 1243–1248.
[136] P. Resnick, et al., The social cost of cheap pseudonyms, J. Econ. Manage. Strat. 10 (2) (2001) 173–199.
[137] C. Duma, N. Shahmehri, G. Caronni, Dynamic trust metrics for peer-to-peer systems, in: Database and Expert Systems Applications, 2005. Proceedings. Sixteenth International Workshop on, 2005, pp. 776–781, doi:10.1109/DEXA.2005.80.
[138] N. Saini, A. Chaturvedi, R. Yadav, Identifying. collusion attacks in p2p trust and reputation systems, Int. J. Comput. Appl. (IJCA) 2 (2014) 36–41.