Hindawi
Mathematical Problems in Engineering
Volume 2018, Article ID 5636319, 8 pages
https://doi.org/10.1155/2018/5636319

Research Article

A Modified Bayesian Trustworthiness Evaluation Method to Mitigate the Effect of Unfair Ratings

Manawa Anakpa, Yuyu Yuan, and Ghazaros Barseghyan

Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, School of Software, Beijing University of Posts and Telecommunications, 10 Xitucheng Road, Haidian District, Beijing 100876, China

Correspondence should be addressed to Manawa Anakpa; anakpa@yahoo.fr

Received 4 July 2017; Revised 31 October 2017; Accepted 10 December 2017; Published 14 May 2018

Academic Editor: Rattikorn Hewett

The choice of trustworthy interaction partners is one of the key factors for successful transactions in online communities. To choose the most trustworthy sellers to interact with, buyers rely on trust and reputation models. Therefore, online systems must be able to accurately assess peers' trustworthiness. The Beta distribution function provides a sound mathematical basis for combining feedback and deriving users' trustworthiness. But the Beta reputation system suffers from many forms of cheating behavior such as the proliferation of unfair positive ratings, leading a poor service provider to build a good reputation, and the proliferation of unfair negative feedback, leading a good service provider to end up with a bad reputation. In this paper, we propose a new and coherent method for computing users' trustworthiness by combining the Beta trustworthiness expectation function with the credibility function. This novel combination mechanism mitigates the impact of unfair ratings. In comparison with Bayesian trust model, we quantitatively show that our approach provides significantly more accurate estimation of peers' trustworthiness through feedback gathered from multiple sources. Furthermore, we propose an extension of Bayesian trustworthiness expectation function by introducing the initial trust propensity to allow assessing individuals' initial trust.

1. Introduction

Social networks and e-commerce platforms are developed to enable social actors to share information and develop lucrative activities. These platforms have been successful in terms of security, but their openness and their ability to accommodate a large number of players make them vulnerable due to the proportionate number of malicious users that is associated. If the Public Key Infrastructure (PKI) has been designed to address key management issues, it has also created trust management problems. Indeed, the certificates provide information about the identity of actors without giving any information about their behavior. In addition, an actor may change his name or profile so that others will never recognize him as a malicious user. This has increased uncertainty among partners in peer community networks. As in [1], we argue that certificates alone are not enough and that we must also take into account the behavior of all participants in opportunistic networks such as social networks and e-commerce platforms. Currently, many researchers are focused on developing new techniques that address both device performance and users' behavior.

The information society technologies should be able to accurately track the behavior of its users and make fair recommendations, warning, and sanction decisions depending on the context and the level of damage caused by any malicious user. To do so, we propose an adaptive evidence gathering mechanism that makes use of all the available information, that is, both positive and negative evidence, both from individual and collective experience. In order to reduce the impact of unfair ratings (both positive and negative) faced by Bayesian reputation systems, a novel trust evaluation model is proposed for quantifying users' trustworthiness.

This paper is organized as follows. Section 2 presents the related work. In Section 3, we describe the system and explain how feedback (or evidence) is collected and updated. In Section 4, the Bayesian trust model and its weaknesses are presented, and solutions are proposed to overcome these weaknesses. In Section 5, we propose an extension of Bayesian trustworthiness expectation function by introducing the

initial trust parameters that allow assessing individuals' initial disposition to trust, and furthermore, we propose a modification of Bayesian trustworthiness evaluation method for mitigating the impact of unfair feedback, both positive and negative. The experiments comparing our approach to the Bayesian standard trustworthiness method for the scenarios of receiving unfair ratings are presented in Section 6. Finally, a short conclusion is given in Section 7.

2. Related Work

In a virtual world such as e-commerce marketplace, users can neither physically verify the quality of the exchange products before buying them, nor ensure the security of personal data, which creates an uncertainty and mistrust between the actors of the same network [2]. The growing uncertainty over the Internet is a critical obstacle to the success of transactions in the network [3], and it has been a concern of many researchers and practitioners who have suggested that trust is one of the critical factors that impact the success of virtual communities, especially, electronic commerce [4].

Trust systems have been proposed by many practitioners and researchers for a variety of applications, among them are the selection of trustworthy peers in a peer-to-peer network, the choice of good transaction partners for online auctioning such as E-bay, and the detection of misbehaving nodes in mobile ad hoc networks [5]. There is a trade-off between efficiency in using all the available information from both direct and indirect experience and robustness against false ratings [6]. If the feedback provided by others is considered, the trust evaluation system can be vulnerable to false praise and false accusations. However, if only one's own experience is considered, then the relevant experience made by others remains unused. The use of only positive or only negative ratings makes the system susceptible either to false praise or false accusations accordingly.

The Bayesian trust model is one of the most popular trust models in the literature. This model has seduced many researchers [7–11] and practitioners for its simplicity and mathematical foundation. In addition, the Bayesian trust model takes into account both positive and negative information. It is a well-adapted model for deriving trustworthiness expectation of an entity based on the evidence collected from the past interactions, either individual or collective [12]. The work presented in [13] shows that the Bayesian model lacks the subjectivity and can be extended by introducing context-dependent parameters such as the initial disposition to trust. This subjective approach of trust is congruent with the definitions of trust provided in [14, 15]. Indeed, trust is the subjective expectation of an entity about the future actions of another based on the past observations (direct and indirect experience) of others [16, 17].

As in [13], this article focuses on the assessment of online users' trustworthiness by combining evidence provided by different sources. Instead of using the Beta distribution function to compute individuals' global trustworthiness, which opens the door to malicious behavior, this article offers a consistent method to fairly compute entities' trustworthiness through evidence gathered from different sources.

3. System Description and Evidence Collecting

3.1. A Brief Description of the System. In this section, we give a brief description of the model. It should be noted that our proposed trust model is a modification of the Bayesian trust model. Let $N = \{1, 2, \ldots, n\}$ denote the set of n users or peers in online community, and let $i, j \in N$ be two interaction partners in the community. We define two categories of participants, namely, the service provider (seller) i and the client (buyer) j. Each service provider can be considered as a potential evaluator for another target entity, since the former can ask for service from the later and conversely. We assume that every actor in community N can assess the trustworthiness of others in the system, based on direct and/or indirect experience. In order to assess the trustworthiness of the service provider, a trustor maintains the outcome of each interaction as he/she perceives it. At the same time, the trustee may assess the credibility behavior of an evaluator by recording his honesty evaluation at each interaction. For this reason, we propose that bilateral interactions in which both partners have mutual assessment obligations can be considered as two separate interactions where each actor is both an observer and a target element.

3.2. Collecting and Updating Evidence. We must keep in mind that the actors are unknown to each other and they are engaged in an interdependent relationship where some provide services that others consume. That said, the interactions are based on mutual trust built up over time by the partners. So it is important that each actor maintains the outcomes of past interactions with other actors in the system.

For easily integrating evidence derived from feedback of past interactions between users, we propose that each feedback score is a value θ in the range $[-1, 1]$, where the lowest value ($\theta = -1$) expresses an interaction resulting in a total disappointment or dissatisfaction and the highest value ($\theta = 1$) expresses a total satisfaction of an actor after an interaction takes place. We think that an observer i may have different parameter θ for every interaction partner j and for each kth transaction. Thus, this parameter should be indexed by i, j, and k.

Suppose that, after each kth transaction, a peer i receives the θ_{ij}^k score from a peer j. Then, the couple (r_{ij}^k, s_{ij}^k) of satisfactory r_{ij}^k and unsatisfactory s_{ij}^k ratings is generated by $r_{ij}^k = v(1 + \theta_{ij}^k)$ and $s_{ij}^k = v(1 - \theta_{ij}^k)$ formulas. In other words, the parameters r_{ij}^k and s_{ij}^k are the amounts of satisfaction and dissatisfaction the peer j has with the peer i for each kth transaction, respectively. It is worth noting that each value of the couple (r_{ij}^k, s_{ij}^k) belongs to the set $[0, 1]$. Thus, the total amount of satisfaction $r_{ij}(I_{ij})$ and dissatisfaction $s_{ij}(I_{ij})$ of the peer j towards peer i after I_{ij} transactions will be

$$r_{ij}\left(I_{ij}\right) = v\sum_{k=1}^{I_{ij}}\left(1 + \theta_{ij}^k\right),$$
$$s_{ij}\left(I_{ij}\right) = v\sum_{k=1}^{I_{ij}}\left(1 - \theta_{ij}^k\right), \quad (1)$$

where the parameter v is nothing other than the weight of the derived evidence as introduced in [8]. The importance and the impact of this parameter are no longer to be demonstrated and to facilitate our experiments, we have set the value of v to 0.5. It should be noted that, even if the approach is capable of handling continuous evidence ($\theta \in [-1, 1]$), the binary evidence only ($\theta \in \{-1, 1\}$) is considered in this paper. Furthermore, assuming that the total amount of satisfaction and dissatisfaction a peer j has with peer i after I_{ij} transactions is $r_{ij}(I_{ij})$ and $s_{ij}(I_{ij})$ respectively, after $I_{ij} + 1$ transactions, the updated total amount of satisfaction $r_{ij}(I_{ij} + 1)$ and dissatisfaction $s_{ij}(I_{ij} + 1)$ the peer j has with peer i is given by

$$\begin{aligned} r_{ij}\left(I_{ij}+1\right) &= r_{ij}\left(I_{ij}\right) + v\left(1+\theta_{ij}^{I_{ij}+1}\right), \\ s_{ij}\left(I_{ij}+1\right) &= s_{ij}\left(I_{ij}\right) + v\left(1-\theta_{ij}^{I_{ij}+1}\right). \end{aligned} \tag{2}$$

In our approach, we propose that each client continuously maintains the two amounts of evidence (r_{ij}, s_{ij}) (I_{ij} is omitted for brevity) obtained after a sequence of interactions with each of its service providers in the P2P network. Conversely, each service provider holds a pair of praise and complaint (p_{ij}, c_{ij}) (I_{ij} is omitted again for brevity) values during interactions with his clients, which are calculated analogous to (r_{ij}, s_{ij}). Furthermore, we assume that an opinion about a target entity i is an aggregation of (r_{ij}, s_{ij}) provided by all of its interacted peers j in P2P network, and for more accuracy in assessing the behavior of a target peer i, it is necessary to collect a relatively large amount of evidence about that service provider taking into account the credibility of each of its raters computed using (p_{ij}, c_{ij}) pairs. We argue that the more evidence becomes available, the more people become enlightened and more certain about the behavior of their interaction partners.

4. Trust Computation

Trust is a subjective and complex concept that is difficult to assess with multiple factors of different degrees of importance that intervene in its construction. One of the most important factors of trust towards an entity is his reputation that involves subfactors such as competence, reliability, and credibility. Additional subfactors can be associated depending on the context; see [18] for more information about trust attributes. In our approach, we assume that a higher reputation induces more trust and conversely. In other words, an entity with a higher reputation will be considered more trustworthy. Thus, computing the degree of trustworthiness of entities in online community is a simple and fair way of assessing trust of their interaction partners. This will help sort the nodes, from good to bad, and make recommendations accordingly. In the following subsections, we first present the Bayesian representation of trust and its weaknesses, and then we propose solutions and a mathematical method to model users' trustworthiness based on the evidence provided by their interaction partners.

4.1. Bayesian Representation of Trust. Our trustworthiness representation is based on the Beta probability density function presented in [8], which is suitable for representing binary events. Indeed, Bayesian inference is an important method in mathematical statistics and the Beta probability density function provides a sound mathematical basis for a simple and flexible estimation of trustworthiness ratings from a collection of evidence. As more evidence or information becomes available, Bayes' theorem is used to update the probability for a hypothesis. Indeed, an observer may believe that there is a probability p defined on the interval $[0, 1]$ such that a given target entity acts honestly without betraying, and simultaneously, there is a probability $1 - p$ such that the target entity misbehaves during an interaction. The parameters p are random variables, and each observer models the uncertainty by assuming that each random variable p itself is drawn according to a prior distribution that is updated as new observations become available. This is how the Bayesian standard framework works. Furthermore, the Beta distribution is a family of continuous probability distributions defined on the interval $[0, 1]$ parametrized by two positive shape parameters, denoted by α and β, which appears as exponents of the random variable and control the shape of the distribution.

The original Beta probability density function (Beta-PDF) denoted by $f(p \mid \alpha, \beta)$ is expressed using the gamma function Γ as follows:

$$f\left(p \mid \alpha, \beta\right) = \frac{\Gamma\left(\alpha+\beta\right)}{\Gamma\left(\alpha\right)\Gamma\left(\beta\right)} p^{\alpha-1}\left(1-p\right)^{\beta-1}, \tag{3}$$

where $0 < \alpha$, $0 < \beta$, and $p \in [0, 1]$, such that the probability variable $p \neq 0$ if $\alpha < 1$, and $p \neq 1$ if $\beta < 1$.

The associated posterior trustworthiness expectation function denoted by $E(\alpha, \beta)$ is defined as follows [8, 15]:

$$E\left(\alpha, \beta\right) = \frac{\alpha}{\alpha+\beta}. \tag{4}$$

By setting the parameters $\alpha = 1 + \sum_{j=1}^{n_i} r_{ij}$ and $\beta = 1 + \sum_{j=1}^{n_i} s_{ij}$, where n_i represents the peer i's total number of evaluators, the traditional (standard) Bayesian approach evaluates the trustworthiness τ_i^{standard} of the peer i based on the following formula:

$$\tau_i^{\text{standard}} = E\left(r_{ij}, s_{ij}\right) = \frac{1 + \sum_{j=1}^{n_i} r_{ij}}{2 + \sum_{j=1}^{n_i}\left(r_{ij} + s_{ij}\right)}. \tag{5}$$

4.2. The Weaknesses of Bayesian Model. In this section, we have enumerated some weaknesses of Bayesian trust model. In addition, we explained the necessity of introducing new parameters and show their impact on users' trust behavior.

4.2.1. The Lack of Subjectivity. Most of the existing trust models use the uniform distribution Beta(1, 1) as the prior trustworthiness value assigned initially to each target entity when there is no information or evidence available to support a hypothesis. We argue that, by considering the initial trustworthiness value as being uniform for any beginner in the system, the Bayesian standard model lacks realism with

respect to the subjectivity view of trust. Moreover, we argue that the associated expectation value $E(1,1) = 0.5$ assigned initially to each beginner in the Bayesian standard model is unfair because a malicious actor whose reputation rating falls below 50% ($E(\alpha, \beta) < 0.50$) will find it more advantageous to abandon his current account and reenter the system in order to get the prior trustworthiness value ($E(1,1) = 0.5$).

4.2.2. The Vulnerabilities of the Bayesian Model. In the Bayesian trust and reputation model, trust is based essentially on the reputation that each actor builds as he interacts with other actors in the system. This trust evaluation model merely aggregates the binary feedback scores collected from peers. But sources of information are not always credible. We argue that trust systems that rely on the Bayesian standard trust model are flawed in several ways. Indeed, the Bayesian standard trust model is exposed to the following cheating behaviors:

(i) The proliferation of unfair positive ratings: a service provider may corrupt a handful of evaluators through profit-sharing so that they evaluate positively the service offered, even if the service is of poor quality, leading an untrustworthy actor to end up getting a large number of false positive statements.

(ii) The proliferation of unfair negative feedback: a peer can be a victim of false judgments; in this case, an unlucky service provider comes to interact with a handful of malicious peers who always accuse others by falsely claiming that they provide poor service, leading a trustworthy actor to end up getting a large number of false negative statements.

Bayesian trust model is susceptible to all of these problems. To overcome these issues, we introduce new parameters and we propose a consistent method to fairly compute user's trustworthiness.

4.3. Proposed Solutions

4.3.1. Overcoming Initial Trust Problem. As outlined in Section 4.2.1, the Bayesian standard model lacks realism with respect to the subjectivity view of trust and opens the door to several types of malicious behavior in the peer community. Thus, instead of using the traditional uniform distribution, Beta(1, 1), and its associated expectation value, $E(1,1) = 0.5$, to compute the prior trustworthiness of each beginner in the absence of evidence, we introduce a new parameter called trust propensity to allow each observer to express personal disposition to trust before any prior interaction with an unknown target entity. The trust propensity is a subjective and context-dependent parameter. For example, an observer's trust propensity with an unknown entity in a file-sharing scenario might be higher, but this might be not true for online shopping or online medical advice. The benevolence, the expertise, the context, and other factors (see [18]) are trust attributes that affect highly human mind.

4.3.2. Overcoming Unfair Ratings. Even if the problem of unfair feedback, both positive and negative, seems unsolvable due to the subjective nature of peers' behavior (i.e., the probability of performing a particular action depends on personal characteristics), we can develop strategies to deter malicious users and also minimize the impact of the unfair judgments they provide.

First, we propose a mechanism for gathering evidence, where the two parties (service provider and client) rate each other. On the one hand, customers have the opportunity to evaluate service providers through the quality of their services after each interaction; on the other hand, service providers have the opportunity to report the dishonest behavior of malicious evaluators. This mechanism is similar to a game, where each party will seek to cooperate with the other in order to avoid tensions that could bring down the reputations of both parties.

Secondly, we propose a simple trustworthiness computation model in which individuals make choices by weighting the impact of their decisions on themselves and others. The new trustworthiness rating function is an extension of the Bayesian standard trustworthiness expectation function. This was possible by integrating each evaluator's credibility rating into the trustworthiness expectation function presented in [7–11].

4.3.3. Integration of New Parameters. Similar to [13, 15], we introduced the parameters r_{ij}^0 and s_{ij}^0 for expressing player j's prior knowledge about player i. These two parameters are, respectively, known as player j's prior believe and prior disbelieve, and they allow introducing another parameter $\theta_{ij}^0 \in [-1, 1]$ known as player j's trust propensity. For more details on trust propensity, see [19–21]. This leads us to define two important concepts: initial belief and initial disbelief.

Definition 1 (initial belief and disbelief). Initially (before any interaction happens between two peers), a service consumer (peer j) may naturally assume that there exists a parameter $\theta_{ij}^0 \in [-1, 1]$ so that the service provider (peer i) will act honestly, based solely on its personal characteristics. Then, the parameters r_{ij}^0, respectively, s_{ij}^0, called peer j's initial belief, respectively, initial disbelief, are defined as follows:

$$r_{ij}^0 = \frac{1 + \theta_{ij}^0}{2}, \qquad s_{ij}^0 = \frac{1 - \theta_{ij}^0}{2}, \tag{6}$$

where, $i, j \in N$, and $N = \{1, 2, \ldots, n\}$ is the set of peers. Another trust factor introduced in this model is the credibility w of each evaluator which is defined as follows.

Definition 2 (credibility). Let $c_j(I_j)$ represent the total number of complaints a client j receives from all of its n_j interaction partners after $I_j = \sum_{i=1}^{n_j} I_{ij}$ transactions. The parameter $w_j(I_j)$, defined by

$$w_j\left(I_j\right) = 1 - \frac{c_j\left(I_j\right)}{I_j}, \tag{7}$$

is peer j's credibility, where $I_j \geq 1$ and $w_j(I_j) \in [0,1]$. Later we will use c_j and w_j instead of $c_j(I_j)$ and $w_j(I_j)$ accordingly for the brevity.

5. Extending Bayesian Trust

Let $N_i = \{1, \ldots, n_i\}$, $N_i \subset N$ be the set of n_i evaluators of peer i. The couple (r_{ij}, s_{ij}) of positive r_{ij} and negative s_{ij} feedback that have been collected from the peer j's individual experience with the peer i are the main parameters used to compute the degree of trustworthiness of the target entity i in this model. Therefore, we compute the expected posterior trustworthiness value of the peer i using the parameters $\alpha_{\text{mod}} = r_{ij}^0 + r_{ij}$ and $\beta_{\text{mod}} = s_{ij}^0 + s_{ij}$ defined in the Beta distribution function, and the credibility rating w_j of each source of evidence, where r_{ij}^0 and s_{ij}^0 represent the initial trust parameters of an individual as defined above (see (6)).

If we consider r_{ij} and s_{ij} as the total number of positive and negative feedback, respectively, received by peer i from peer j after I_{ij} interactions, then i's modified posterior trustworthiness expectation value recorded by peer j can be denoted by E_{ij} and defined as follows:

$$E_{ij} = \frac{r_{ij}^0 + r_{ij}}{r_{ij}^0 + s_{ij}^0 + r_{ij} + s_{ij}}, \tag{8}$$

where r_{ij}^0 and s_{ij}^0 denote the initial belief and the initial disbelief, respectively, and $E_{ij} \in [0,1]$. Now that the ingredients are gathered, we can define the trustworthiness rating of each peer i in the network.

Definition 3 (trustworthiness rating). Let $N_i = \{1, \ldots, n_i\}$, $N_i \subset N$ be the set of n_i evaluators of peer i. Let w_j be the peer j's credibility given by (7), and let E_{ij} be the peer i's trustworthiness expectation value provided by peer j and defined by (8); the peer i's trustworthiness rating τ_i is defined as follows:

$$\tau_i^{\text{mod}} = \frac{1}{n_i} \sum_{j=1}^{n_i} w_j E_{ij}. \tag{9}$$

Note that the trustworthiness rating τ_i^{mod} is a value between 0 and 1. As a matter of fact, τ_i^{mod} is the aggregation of the trustworthiness expectation values built based on the provided ratings by each evaluator of the peer i.

In contrast, the traditional (standard) Bayesian approach evaluates the trustworthiness of the peer i based on (5).

6. Experiments

Similar to [22], the experiments are conducted on a variety of P2P networks which are simulated with maximum number of 32, 64, and 128 users. 80% of the population consists of clients and the rest consists of service providers. The number of maximum interactions between a pair of client and service provider is set to 1.5 × (population size). Interactions are created randomly for connecting clients to service providers.

Table 1: An example record.

Client Id	Service provider Id	r	s	p	c	I
3	7	0	2	1	1	2
1	6	6	1	7	0	7
4	5	1	4	0	5	5
3	6	2	6	5	3	8
2	7	4	2	5	1	6
4	7	5	1	2	4	6

The experiments are performed from a time t and contain records of transactions rating information. An example of records table is given in Table 1.

ClientId and *ServiceProviderId* fields are self-descriptive, I is the total number of interactions between a pair of client and service provider, r and s are the number of positive and negative feedback accordingly, given by the client to the service provider, and p and c are the number of praise and complaints coming from a service provider to the client accordingly. The following scenarios are considered.

In all of the figures discussed below, the formula to compute the trustworthiness of a peer i in case of the traditional (standard) Bayesian method is given by (5) (see Section 4.1) and in case of our proposed modified Bayesian approach the formula is presented by (9) (see Section 5).

The first case (Figures 1, 2, and 3) is devoted to observe the impact of a large amount of unfair positive ratings from a client. In order to accomplish the task, a service provider (seller) is chosen from the network that has no very high reputation and among his credible clients (buyer) one is chosen that is going to give only positive feedback for all of the next interactions. So, the client will also receive only praise ratings from the service provider. In order to observe the dependency of the evaluated trustworthiness of the service provider from the client's feedback, other clients are not interacting with him after time t. Our method is compared with the traditional (standard) Bayesian method to measure the trustworthiness of the service provider after time t.

Figures 1, 2, and 3 are presented for a randomly initiated P2P network where total number of users are 32, 64, and 128 accordingly.

From Figures 1, 2, and 3, it can be seen that our method is more robust against unfair positive feedback from a client compared to the traditional Bayesian method. Indeed, after the growing number of positive feedback, the perceived trustworthiness of the service provider, calculated by our approach, stops growing in practice, and the further corruption of the client is becoming useless. In contrast, using Bayesian traditional method, the trustworthiness of the service provider is enhanced significantly and tends to 1.

The second scenario explores the influence of giving unfair negative feedback to a reputable service provider. As mentioned in Section 4.2.2, this can happen when a competitor registers in the system as a client and tries to bring down the business of his college. It can also happen when a buyer colludes with a seller to badmouth the seller's competitors, resulting in gains to the seller. A reputable

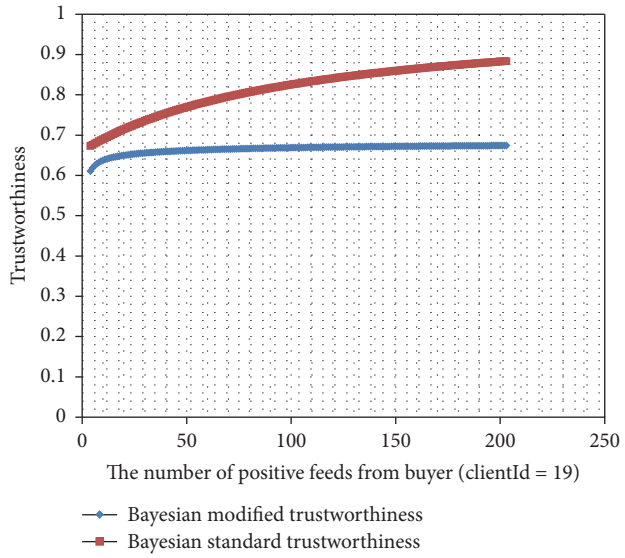

Figure 1: The impact of false praise from client (clientId = 19) on the trustworthiness of the service provider (serviceProviderId = 30).

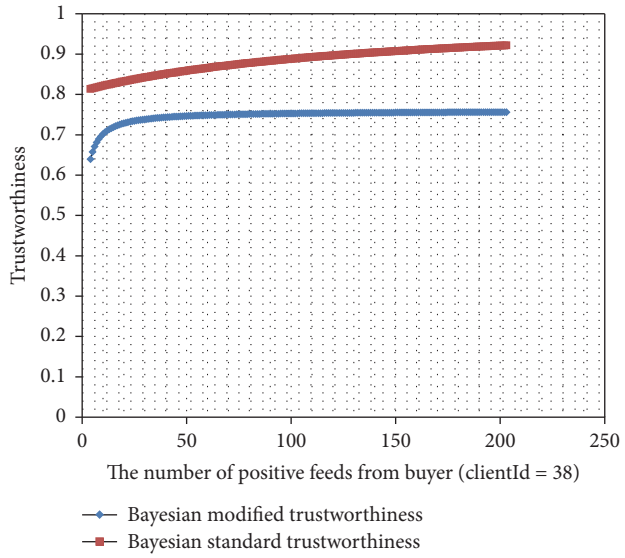

Figure 2: The impact of false praise from client (clientId = 38) on the trustworthiness of the service provider (serviceProviderId = 63).

service provider is chosen from a simulated network at a time t, and one of his less active clients (the precondition that the client just starting the slandering attack) is chosen to start misbehaving. From that time, interactions are only between this pair of users. Other clients do not interact with the service provider for the same reason as in the first scenario. Figures 4, 5, and 6 are presented for randomly initiated networks where total number of users is 32, 64, and 128 accordingly.

From Figures 4, 5, and 6, it can be seen that our method mitigates the slandering attacks from the client compared to the traditional Bayesian approach and the measured trustworthiness of the service provider does not reduce much after the growing number of negative feedback from the

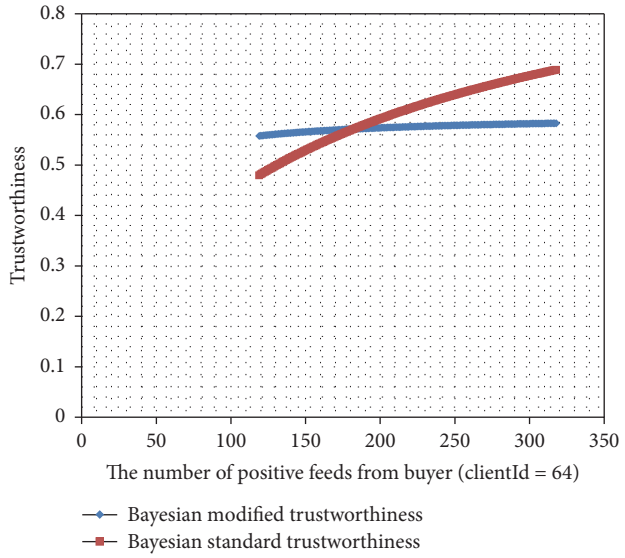

Figure 3: The impact of false praise from client (clientId = 64) on the trustworthiness of the service provider (serviceProviderId = 111).

client. Furthermore, the reducing speed is also decreasing and after some point it stops practically.

In all of Figures 1–6, at the time t the curve of Bayesian traditional method and our approach starts from different trustworthiness scores owing to the different prior parameters r and s. As mentioned before, when there is no interactions, the standard Bayesian approach assigns the value 0.5 to the prior trustworthiness expectation. Moreover, all of the clients are assumed to be equally credible while giving their ratings. As a result, in most cases standard Bayesian trustworthiness assessment method is more sensible to both positive and negative feedback. In contrast, our method enables us to define the initial trust parameters r and s subjectively. In the experiments the values are given pseudo randomly, so, in some cases at the time t our approach can evaluate the trustworthiness of an observed service provider higher (Figures 3 and 5) or lower (Figures 1, 2, 4, and 6) compared to the standard Bayesian method. In fact, in all of the cases our method is more resistive to growing number of both positive and negative feedback.

The experiments are conducted on many datasets and only few figures are presented. The source code in Java and the simulated networks in .xlsx extension can be found in [23]. Figures 1, 2, and 3 are based on records131.xlsx, records132.xlsx, and records19.xlsx accordingly, and Figures 4, 5, and 6 are from records130.xlsx, records67.xlsx, and records125.xlsx accordingly.

7. Conclusion and Future Work

In sum, due to the problems concerned with the standard Bayesian trustworthiness evaluation approach such as vulnerability to unfair ratings, both positive and negative, in the case of having a low trustworthiness value, a malicious service provider will find it advantageous to reenter the system to return the initial higher trustworthiness expectation value

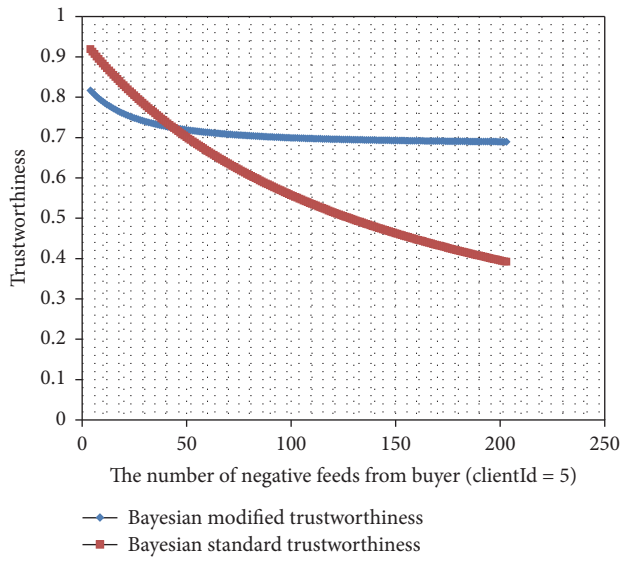

Figure 4: The impact of false complaints from client (clientId = 5) on the trustworthiness of the serviceProvider (serviceProviderId = 26).

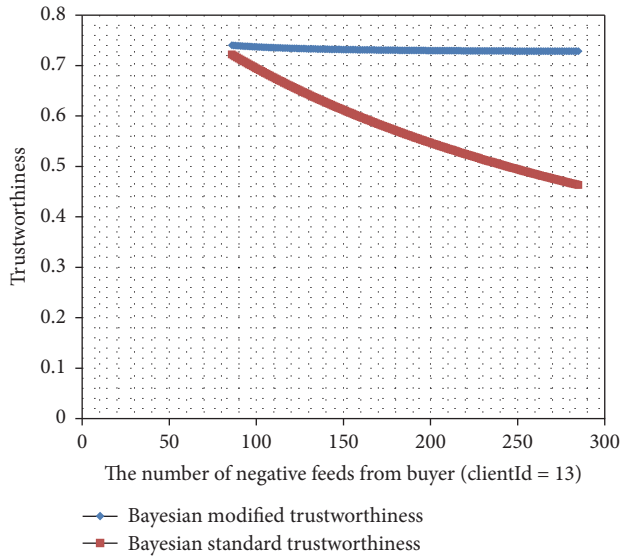

Figure 5: The impact of false complaints from client (clientId = 13) on the trustworthiness of the serviceProvider (serviceProviderId = 52).

0.5; therefore, we propose a novel modified Bayesian trustworthiness evaluation method to overcome these problems.

We claim the necessity of giving bidirectional ratings in P2P networks. In this way, based on the ratings elicited from service providers the credibility of each of their clients is computed. Then, the trustworthiness scores of the service providers are calculated taking into account the credibility of each of their evaluators. As a matter of fact, the performed experiments have shown that our proposed approach performs better while dealing with unfair ratings, both positive and negative, compared to the traditional Bayesian trustworthiness method in the discussed scenarios. Thus, our

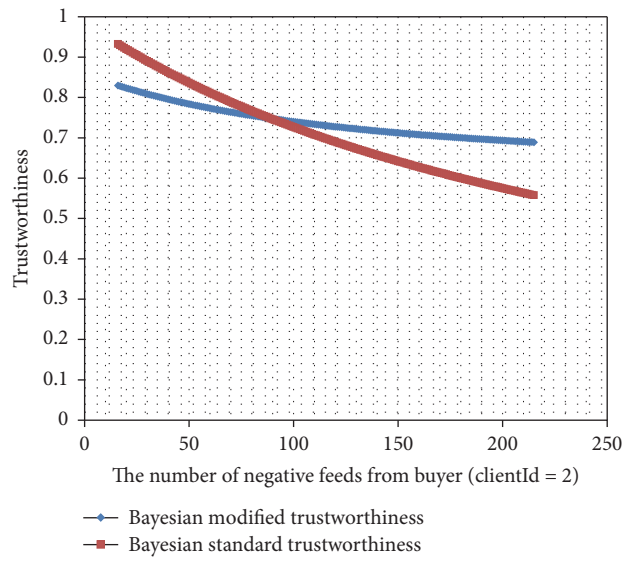

Figure 6: The impact of false complaints from client (clientId = 2) on the trustworthiness of the serviceProvider (serviceProviderId = 96).

mechanism enables us to diminish the influence of these ratings significantly. In addition, by considering the initial trust to be subjective, we give more flexibility to model the client's initial trust with its further dynamic changes and make it useless to reenter the system by expecting to have a higher initial trustworthiness. As a result, our method is more resistive against these abovementioned problems than the standard Bayesian trustworthiness approach.

In future works, we are going to discuss how to integrate an aging factor in our method because users may change their behavior over time; therefore, it is desirable to define a way to give greater weights to more recent ratings. Moreover, we will observe techniques to detect malicious users and approaches to treat them. Thus, by tackling the problem by more ways, the behavior of untrustworthy peers can be handled better; as a consequence, we can improve the performance of our approach.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (no. 91118002).

References

[1] V. Cahill, E. Gray, J.-M. Seigneur et al., "Using trust for secure collaboration in uncertain environments," *IEEE Pervasive Computing*, vol. 2, no. 3, pp. 52–61, 2003.

[2] M. K. O. Lee and E. Turban, "A trust model for consumer internet shopping," *International Journal of Electronic Commerce*, vol. 6, no. 1, pp. 75–91, 2001.

[3] A. F. Salam, L. Lyer, P. Palvia, and R. Singh, "Trust in e-commerce," *Communications of the ACM*, vol. 48, no. 2, pp. 72–77, 2005.

[4] M. J. Bitner, "Servicescapes: The Impact of Physical Surroundings on Customers and Employees," *Journal of Marketing*, vol. 56, no. 2, pp. 57–71, 1992.

[5] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of nodes: fairness in dynamic ad-hoc networks)," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '02)*, pp. 226–236, June 2002.

[6] S. Buchegger and J. Y. Le Boudec, *The effect of rumor spreading in reputation systems in mobile ad-hoc networks*, Sofia-Antipolis, Wiopt'03, March 2003.

[7] S. Buchegger and J.-Y. Le Boudec, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Communications Magazine*, vol. 43, no. 7, pp. 101–107, 2005.

[8] A. Josang and R. Ismail, "The beta reputation system," in *In Proceedings of the 15th Bled Conference on Electronic Commerce*, 2002.

[9] L. Mui, M. Mohtashemi, C. Ang, P. Szolovits, and A. Halberstadt, "Ratings in distributed systems: A bayesian approach," in *Workshop on Information Technologies and Systems*, 2001.

[10] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, "TRAVOS: trust and reputation in the context of inaccurate information sources," *Autonomous Agents and Multi-Agent Systems*, vol. 12, no. 2, pp. 183–198, 2006.

[11] A. Whitby, A. J. sang, and J. Indulska, "Filtering out unfair ratings in bayesian reputation systems," *The Icfaian Journal of Management Research*, vol. 4, no. 2, pp. 48–64, 2005.

[12] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[13] S. Ries, "Extending Bayesian trust models regarding context-dependence and user friendly representation," in *Proceedings of the 24th Annual ACM Symposium on Applied Computing (SAC '09)*, pp. 1294–1301, ACM Press, March 2009.

[14] D. Gambetta, "Can we trust trust?" in *Trust: Making and Breaking Cooperative Relations, electronic edition*, D. Gambetta, Ed., chapter 13, pp. 213–237, 2000.

[15] A. Josang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 3, pp. 279–311, 2001.

[16] S. Schmidt, R. Steele, T. S. Dillon, and E. Chang, "Fuzzy trust evaluation and credibility development in multi-agent systems," *Applied Soft Computing*, vol. 7, no. 2, pp. 492–505, 2007.

[17] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model of trust and reputation," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pp. 2431–2439, Big Island, Hawaii, USA, 2002.

[18] M. Anakpa and Y. Yuan, "Multidisciplinary Trust Conceptualization: A General Model for Customer Trust Building in e-Commerce," *Communications in Computer and Information Science*, vol. 426, pp. 366–373, 2014.

[19] H. W. Kee and R. E. Knox, "Conceptual and methodological considerations in the study of trust and suspicion," *Journal of Conflict Resolution*, vol. 14, no. 3, pp. 357–366, 2016.

[20] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review (AMR)*, vol. 20, no. 3, pp. 709–734, 1995.

[21] D. H. McKnight, L. L. Cummings, and N. L. Chervany, "Initial trust formation in new organizational relationships," *Academy of Management Review (AMR)*, vol. 23, no. 3, pp. 473–490, 1998.

[22] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities," in *Proceedings of the IEEE International Conference on E-Commerce, CEC '03*, pp. 275–284, CA, USA, June 2003.

[23] https://github.com/kazaros91/Trustworthiness.