Information Fusion 103 (2024) 102082

Contents lists available at ScienceDirect

Information Fusion

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

A reputation-based trust evaluation model in group decision-making framework

Xinli You [a], Fujun Hou [b,*], Francisco Chiclana [c,d]

[a] School of Economics and Management, Shanxi University, Taiyuan, Shanxi, PR China
[b] School of Management and Economics, Beijing Institute of Technology, Beijing, PR China
[c] Institute of Artificial Intelligence, De Montfort University, Leicester, UK
[d] Andalusian Research Institute on Data Science and Computational Intelligence (DaSCI), University of Granada, Granada, Spain

ARTICLE INFO

Keywords:
Trust credibility
Direct trust feedback
Recommend trust
Reputation
Group decision-making

ABSTRACT

In group decision-making (GDM) problems, experts need to communicate and adjust their opinions in order to achieve consensus on the final decision-making output. Since experts may have conflicting opinions, trust can be critical and an important reference to use in the decision-making process when some experts are required to modify opinions. Recently, decision-making models based on trust and reputation have been investigated intensively. However, these research works usually rely on the constructed social trust network and honesty and fairness of the trust ratings from experts are taken for granted. The objective of this study is to develop a reputation-based trust model for GDM framework to obtain the trust relationship among experts from their direct interaction and word of mouth. First, the paper defines a trust credibility measure to filter out malicious experts before trust assessment, and designs direct trust feedback based on the interaction quality. Then, based on this direct trust feedback, the global reputation model is proposed according to the synthetical performance of received and provided trust feedback, which encourages long-term good behaviour and guarantees trustworthy communications and interactions. The reputation-based trust and direct trust feedback together build trust relationship among experts. Finally, a simulation experimental analysis of the proposed trust and reputation models is carried out to verify their effectiveness in trust and reputation establishment among the experts, even under the presence of malicious ones.

1. Introduction

In recent years, with the rapid development of communication technology and social network, it is more convenient to share information and exchange services, and hence increasing interactions among individuals and resulting in profound and interesting changes in the decision-making environment and individual decision-making behaviour. Trust relationship between decision-makers (DMs) can influence decision making and consensus reaching during the interactive process in group decision-making (GDM) scenarios [1–8]. Since these procedures facilitate DMs to negotiate and reach acceptable agreements, trust relationship management has been adopted by many researchers to design the consensus process [3–8]. For example, Wu et al. [3] put forward an interaction framework to model consensus for GDM problems where individual trust relationship was applied to generate advice; Liu et al. [7] presented a social network trust propagation based consensus model; while Yu et al. [6] proposed a consensus model with voluntary trust loss as the consensus cost.

Generally speaking, trust derives from two ways [9]: One is direct trust that is provided by experts as trusters based on their own knowledge and direct experience through previous interactions; The other way is called reputation that is obtained from other experts' trust rating on target trustees. Obviously, reputation is a component of trust, but it is based on the direct trust rating of other experts, i.e., reputation comes from trust. Direct trust emphasises the ratings of the expert's own views, while reputation is the aggregation of views from other experts in the database [2]. The reputation model is the mechanism to support trust evaluation. If there is just direct trust, trust evaluation model focuses on trust expression and trust rating calculation [4]. When it comes to reputation, the issue of collection and aggregation reputation should be addressed [9]. Then, there will also be a puzzle: some experts may provide dishonest or unfair ratings for their own benefit.

Trust model was originally proposed in the field of computer, and has been widely used and improved in the field of e-commerce, peer-to-peer networks and so on [10–12]. From the discussion above, although

* Corresponding author.
E-mail address: houfj@bit.edu.cn (F. Hou).

https://doi.org/10.1016/j.inffus.2023.102082
Received 7 May 2023; Received in revised form 17 September 2023; Accepted 18 October 2023
Available online 20 October 2023

many trust-based GDM models have been investigated, some problems still remain to be addressed.

(1) In trust-based GDM, individuals are usually assumed to be honest. However, some experts may provide trust ratings with malicious intentions, such as self-promoting, bad-mouthing, and collusion. This issue affects the generating of genuine feedback on interactions [10]. Since this issue is ignored in existing studies [4,6,8], direct trust rating trustworthiness cannot be guaranteed and social trust environment is vulnerable to attack from malicious experts. Therefore, it is necessary to propose an effective method that measures the credibility of experts and punishes dishonest behaviour, so that experts are urged to provide constant authentic trust rating scores.
(2) Trust models like PopTrust [13] and RWTrust [14] are based solely on network topology and are rooted in the current state of the social network, which ignores the historical interactions between experts, and the impact of behavioural changes of the experts. Additionally, there is no mechanism to dynamically update the quality of the trust assessments based on the behaviours of each expert in the network. Therefore, it is necessary to model the trust relationship between experts with trust assessments dynamically updated to reflect the changes over time in the experts' interaction quality.
(3) Many trust propagation methods in the literature [2,4,15,16] are based on social network propagation paths. It is noticed that trust transitivity will be invalid if there are too many expert nodes in the trust chain [17], so a trust propagation method should enable the mediators to connect both the truster and trustee. In addition, the existing trust propagation methods do not focus on the relative importance of mediators, although it is unreasonable to regard the mediators or recommenders as equally important.
(4) There are two main sources of trust degree between experts: direct trust and recommend trust. Thus, a comprehensive trust degree depends on both direct trust and recommend trust. Some existing studies assign weights to direct trust based on the subjective preference of DMs [11,18,19] but fail to reflect the importance of historical interaction experience in their trust evaluation models. Therefore, a new method to derive weights for direct trust and recommend trust is needed to derive experts' comprehensive trust degrees.

Accordingly, this study proposes a trust and reputation model to obtain the comprehensive trust degree between experts based on a trust management system that analyses the related trust characteristics of experts and their interaction behaviours in the context of SC. The main contributions and highlights of this study are summarised as follows:

(1) The trust ratings from experts depend on experts' profiles and opinion similarity, the accuracy of experts' opinions, and the popularity level of each expert. A trust credibility measure of experts is proposed to filter out malicious experts by judging whether the performances of experts beyond trust assessment match their reputation. This method cannot completely exclude all malicious experts from active experts, thus the trustworthiness of trust ratings is proposed to be enhanced with the direct trust feedback by considering the number of interactions and their quality .
(2) A trust evaluation management system is proposed based on direct trust feedback and recommended trust rather than social network topology. Thus, there is no need to construct the social network, which is a fairly large or complex task. The technical implementation of this scenario will allow for the historical interaction performance and behaviour strategies of each expert to be used in the experts' global reputation and the design of direct trust feedback.
(3) A reputation model is developed to represent the relative importance of each expert as a recommender. Regarding trust assessment, each expert holds two roles: the truster role as provider of trust ratings for other experts, and the trustee role as receiver of trust ratings from other experts. As a trustee, an expert's reputation is assumed to be the aggregation result of the corresponding trust ratings from all recommenders, which we term the interaction reputation. As a truster, an expert should provide constant fair trust ratings and his/her behaviour performance is defined as behaviour reputation. To carry out the global reputation successfully, the model not only takes into account the interaction performance and behaviour strategy but the time decay factor as well.
(4) The dynamic change of trust is reflected in the update of trust feedback with new interaction experience and in the increase of comprehensive trust value with an increase of interactions within a period of time. To fully consider the interaction experience of experts, a dynamical weight determination method is introduced on the basis of interactions. As the interactions among experts increase, direct trust feedback becomes more important, and its weight coefficient will grow.

The remainder of the paper is organised as follows: Section 2 reviews literature related to trust, reputation and consensus in GDM. Section 3 introduces the framework of the trust and reputation model in GDM, and the main threats to the process of building trust relationship. Section 4 proposes the trust credibility measure to filter out malicious experts, and the trust rating feedback (direct trust) based on interaction quality. Section 5 proposes the global reputation based on the interaction reputation and behaviour reputation from the truster's and trustee's perspective. Section 6 addresses those cases where no direct interactions between experts exists, and proposes a comprehensive trust using both trust rating feedback (direct trust) and recommend trust (indirect trust). The simulation experiments based on the database are described and discussed in Section 7. Finally, Section 8 concludes this paper and proposes future works.

2. Related work

GDM is a scenario with interactions among multiple experts to obtain a solution [20,21]. In the initial stage of the corresponding GDM process, experts may provide conflicting opinions, which means that a consensus reaching process (CRP) is required to achieve a satisfactory decision outcome for the group [22–25]. Nowadays there is an emergent trend that considers trust relationship in this process by means of feedback mechanism to reach a solution of consensus [3–8,26,27]. Wu et al. [4] defined a uninorm interval-valued trust propagation operator to obtain an indirect trust relationship and generate personalised recommendation advice in consensus process accordingly. Considering the impact of overlapped social trust relationships on CRP, Ji et al. [26] constructed an overlapping community-driven feedback mechanism to guide the inconsistent subgroups for improving consensus. Zha et al. [5] proposed a consensus framework based on opinion dynamics and trust/distrust level evolution in a balanced network. A recent survey [27] proposed there is a lack of necessary tools to calculate dynamic trust and reputation for GDM framework.

Trust is a complex concept from Psychology, Economics, and Sociology perspective, and trust model has been proposed previously for numerous purposes in various environments, such as cognitive science, e-commerce, and information system [10–12]. Trust can be considered as the result of historical interactions between individuals, which is known as the direct experience of the trusters. This interpretation of trust was used by Jøang and Ismail [28] to propose a Beta distribution-based reputation model to measure experts' trustworthiness based on a binary outcome of an interaction; while Griffiths [29] developed a multi-dimensional trust model to evaluate the performance of trustee

based on the likelihood of satisfactory interaction result, the likelihood of interaction result within the expected budget, deadline, and quality.

While direct interaction experience is one of the most relevant information sources for trust assessment, it likely may not always be available. Thus, reputation computation models synthesising various information sources are relevant [30]. A classic example is reputation systems based on the provision of feedback by experts implemented by online business such as eBay. However, voluntary feedback cannot guarantee quality of information [31]. Inherent disadvantages and actual threats attack to reputation systems are discussed in Section 3.2. Nevertheless, computational reputation (model) is an active branch of research, and scholars consider reputation to be a significant contributing factor on trust computation [32–35].

Regarding the trust and reputation in the context of GDM, Tundjungsari et al. [1] suggested the trust and reputation mechanism to choose a supra decision maker to assist other DMs in making judgment and decision; Ureña et al. [2] stated the role of trust propagation and reputation in decision making to reach consensus. Trust and reputation models in consensus process are still in the initial stage, not systematic and in-depth, and it needs to be further researched.

3. Trust and reputation framework in GDM

This section briefly introduces the framework of the trust and reputation model in the GDM, and the main threats to the process of building trust relationships.

3.1. Trust interaction environment

In the GDM context, there is an expert panel, whose members are randomly selected from an expert database, to evaluate decision objects/alternatives. In the GDM process, experts communicate their opinion, and even modify preferences in accordance with the requirement to achieve consensus on the final decision result. Trust plays an important role in the consensus reaching process [2–8]. Thus, this study proposes a trust and reputation model for the construction of a trust evaluation matrix $TM = [T_{ij}]_{N\times N}$ among the considered N experts in the panel. The following conditions are assumed for the trust-forming mechanism in the context of GDM [36]:

(1) Trustee and truster experts are self-interested;
(2) Each truster prefers to interact with the most trustworthy trustee expert;
(3) Each truster provides a trust rating on interaction with trustees after the CRP is completed;
(4) Interactions between experts occur in discrete time steps;
(5) The profile of the expert is useful for predicting future behaviour.

Trust is understood as a firm belief in the reliability, truth, or ability of someone. This study assumes that trust can be measured or evaluated and that different levels of trust exist. Thus, this study proposes the following related concepts:

Definition 1 (*Direct Trust*)**.** Under the premise of direct cooperation between two experts, an expert's direct trust on the other expert is based on the experience of their historical interactions, and can be quantified by some mathematical method.

Definition 2 (*Recommend Trust*)**.** In the absence of direct cooperation between two experts (expert and target expert), an expert's recommend trust is based on the (witness) information and the validity of the evidence provided by recommenders who interact with the target expert, and can be quantified by some mathematical method.

Table 1
Trust rating scores and their semantic.

Trust rating score	Trust degree
(0,0.5)	Completely distrust
[0.5,0.6)	Distrust
[0.6,0.8)	Average trust
[0.8,0.9)	Fairly trust
[0.9,1]	Totally trust

Definition 3 (*Comprehensive Trust*)**.** Based on the direct interaction experience with the target expert and the received recommend trust from other experts on the target expert, Comprehensive trust of an expert on the target expert by aggregating the direct trust and recommend trust by some mathematical method.

Each member of the expert panel is a truster when he/she assesses the competence, and trustworthiness of other members of the expert panel (i.e., trustee or target experts). Equally, each expert is a trustee. Recommenders refer to experts who directly interact with truster's target expert, and they may or may not have interaction(s) with a truster. If there is no historical interaction between the truster and trustee, the truster will initiate a request to recommenders (excludes except himself and the target expert). The recommenders will then return (witness information) to the truster, who will adopt it according to the recommenders' reputation level. Take an assessment mission with five experts for instance, depicted in Fig. 1.

In the GDM problem, the object assessment is a one-time task, but there are various mutual interactions among experts. Reputation is what an expert creates through past actions about its intentions and norms on a global level [12], which reflects the following characteristics:

1. It is expected that there will be additional interactions in the future.
2. Reputation building is based on long-term behaviour, without advantage to newcomers.
3. Robust to malicious experts: malicious behaviours have to be immediately flagged and isolated.

After serving as an evaluation expert, each expert Z^i needs to upload two types of information to the trust management system:

(i) An **decision matrix** for alternatives: $Y^i = [y^i_{pq}]$;
(ii) A **trust rating vector** for the other $n-1$ experts in the same assessing panel at time period s

$$R_i(s) = (r_{i\to 1}(s), r_{i\to 2}(s), \ldots, r_{i\to n-1}(s)) \in (0,1]^{n-1},$$

with semantic meaning given in Table 1. EigenTrust model adopted the two-dimensional trust rating [37], i.e., the trust score either $r_{i\to j} = 1$ or $r_{i\to j} = -1$. In this study, we utilise a multi-dimensional trust rating to represent users' trust degree, which resembles an unbalanced linguistic term set [38] $\{l_0 = Completely\ distrust, l_1 = Distrust, l_2 = Average\ trust, l_3 = Fairly\ trust, l_4 = Totally\ trust\}$.

It is assumed that the trust management system adopts a mixture architecture with the role of administrator in the service of trust propagation and aggregation [39]. In the proposed trust evaluation process, each expert may be either an honest expert or an attacker. In order to identify attacker experts and eliminate the negative effects of their attacks, the system is equipped with a reputation-based trust computation mode, which involves the following stages:

(1) Recording of trust behaviour, i.e., trust rating vector.
(2) Storage of trust behaviour: the information can be stored by the expert itself (distributed) or by a global administrator (centralised).

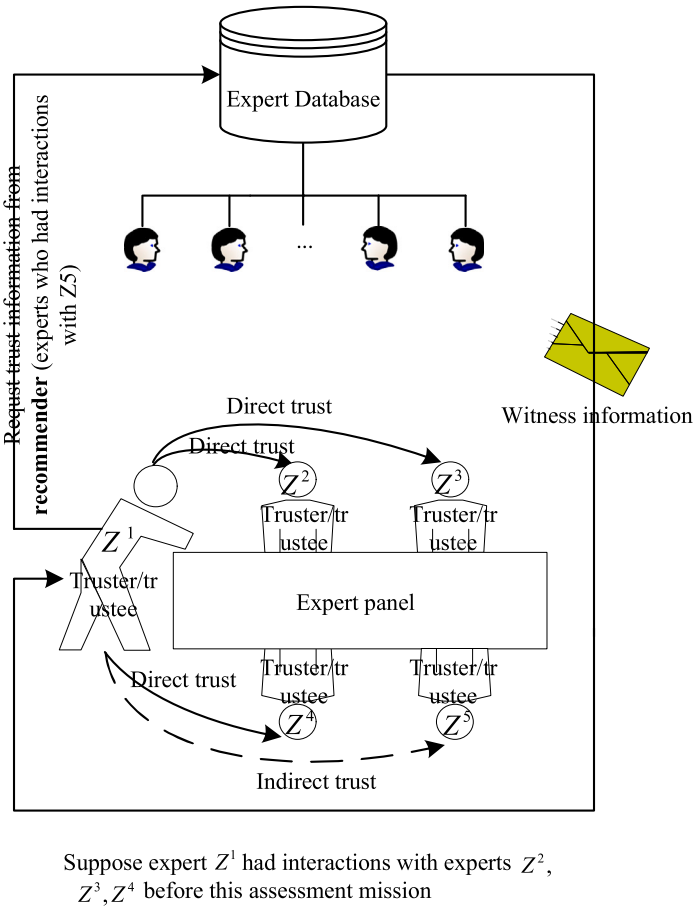

Fig. 1. The visualisation of truster, trustee and recommender.

(3) Assessment of trust behaviour: experts in the expert database are of one of two possible modes: sleep mode and active mode. At time s, an expert is by default on active mode, and selectable by system as an expert to participate in the review process, unless he/she is deemed a malicious expert and is marked on sleep mode until the next time $s+1$.

(4) Recall of trust behaviour: when no direct interaction between experts, a centralised trust manager computes trust evaluation and communicates these to experts. In computing the trust degree between two experts at time s, there are two possible scenarios:

   (i) experts Z^i and Z^j have interacted in the past and their trust ratings are stored in a database;
   (ii) experts Z^i and Z^j have not interacted in the past, then the information sources are other experts' trust rating on Z^i and Z^j, and their own global reputation levels.

3.2. Malicious behaviour

Despite the widespread use and great success of reputation systems, they still may be vulnerable to new and unpredictable malicious behaviour of experts. The below summarises several malicious behaviour and defence methods.

White-washing refers to malicious experts rejoining the system with a new identity to avoid punishment [40]. This attack can be defended by increasing the cost of registration, such that the expert ID is bound to the IP address, real name authentication, and so on. Experts in expert databases require various professional certifications, which can avoid white-washing to some extent.

Traitor (on–off attack) is malicious expert who enhances reputation through good behaviour, then engages in bad rating (attack), and then performs good behaviour after a drop in reputation [28]. To tackle traitor attack, many reputation systems reduce the influence of historical behaviours through the forgetting mechanism. The TrustGuard model calculates experts' reputation based on recent trust feedback [41]; Jøang and Ismail [28] introduced the time decay factor into the Beta distribution-based reputation model to reduce the weight of historical feedback scores; while Sun et al. [42] proposed an adaptive forgetting mechanism that requires long-time interaction and consistent good behaviours to build a good reputation but that a few bad actions can ruin it.

Dishonest rating denotes deliberately false feedback given by a malicious expert for self-promoting, slandering or bad-mouthing, and orchestrating [12]. In order to recognise and deal with these dishonest feedbacks, some methods have been developed: (1) raising the cost of unfair trust ratings, such as certification or real transactions; (2) detecting the dishonest feedback by various techniques, such as clustering method [43], and entropy-based method [44]; (3) mitigating the impact of dishonest feedback, i.e., the given feedback from truster with lower reputation level has less effect on trustee's reputation.

Collusion means conspiracy of a group of experts to artificially boost their reputations by providing high ratings to each other or by degrading other experts' reputations with lower ratings [45]. The existing methods handle this collusion attack by associating the truster's reputation with time factor, such as the time domain analysis [46]. You et al. [45] proposed a transaction

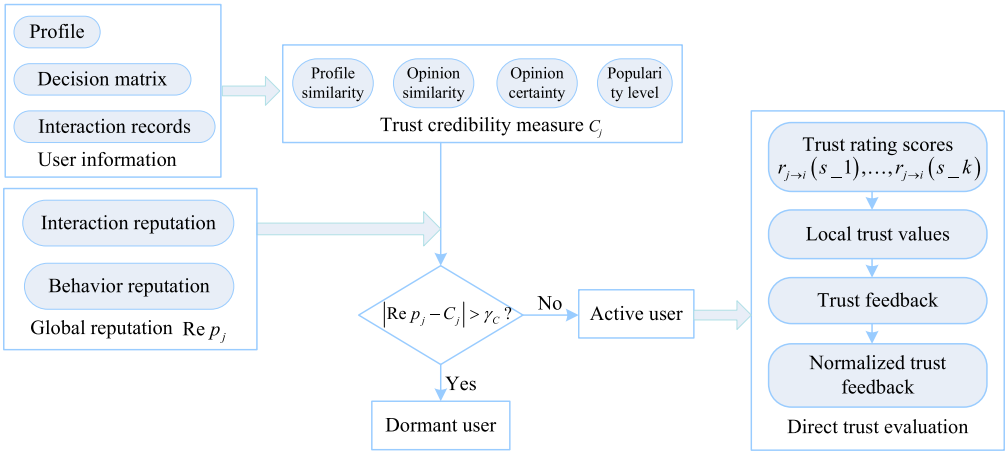

Fig. 2. DTEM main components.

mode for collusion fraud and a recognition method based on a variety of transaction factors, including time and price, using social network analysis and real data of Taobao to verify its identification method.

In summary, existing models utilise the experts' given explicit rating on their interactions to obtain reputation level or direct trust feedback. However, there exist various attacks as above. In online interconnected systems, other resources can be exploited to obtain information about trust and reputation, such as profile similarity and opinion similarity among experts, and their behaviour evolution. In this study, we propose a new trust and reputation model that computes direct trust and reputation-based recommend trust and merges them in an expert-centric influence measure to derive the trust relationship among experts.

4. Direct trust evaluation model

Trust is a dynamic communication rather than a static product and is generated by similar inherent characteristics and numerous interactions among experts. At the initial phase of an assessment decision process, profile similarity of experts may be used as an efficient way to establish trust. As the assessment decision process develops further, individual experts communicate their opinions and learn more about each other, which contributes to the development of trust relations. This study focuses on collecting trust evaluations of experts in the same panel after the assessment decision process to establish a trust foundation for subsequent decision processes.

In the proposed evaluating trust model, direct trust rating or feedback depends on past observed behaviours of experts, while indirect/reputation-based trust evaluation relies on witness information from other experts in the expert database. One of the main novelties of the proposed model in the direct trust evaluation is its trust credibility measure to filter out malicious experts, as shown in Section 4.1. Additionally, this model considers a more realistic scenario where, at any period s, experts may participate in multiple evaluation interactions, $\{s\_k|k = 1,\ldots,K_s\}$. Thus, the proposed direct trust evaluation model (DTEM) is carried out based on the filtered experts and their interaction experience with framework depicted in Fig. 2.

4.1. Trust credibility measure

The quality of a trust system depends on the integrity of the ratings it receives as input. Each expert needs to provide their trust rating scores on other experts after the consensus process. However, there may exist some malicious experts who behave inconsistently when providing their ratings. It is not possible to know malicious expert a priori. In general, it is often the case that honest experts provide their trust ratings taking into account their interactions with other trustees and the performance of trustees. McKnight et al. [47] illustrated the conditions used by individuals to build/develop initial trust in the framework of the theory of reasoned action: competence (ability of the trustee), benevolence (trustee caring and motivation to act in the truster's interests), and integrity (trustee honesty and promise keeping). Based on this principle, a trust credibility measure is investigated to filter out malicious experts before the evaluation process and its effectiveness is illustrated through simulations.

Profile similarity is considered on the basis of successive interaction in the assessment decision process. Profile information refers to some characteristics/features that define unequivocally an expert: gender, age, birthplace, education, work unit, professional title, etc. Profile features (Appendix B) are digitally stored to allow the computation of similarities between experts. During the discussion and negotiation, experts with similar opinions on alternatives are likely to enhance their respective trust in each other, which means that a positive correlation between experts' trust degree and their similarity exists [48]. These similarity measures, considered as external connections, can be used to authenticate the trust rating score to some extent. In addition, the internal sources, information certainty, and activity level of experts, reveal the trustworthiness of trust feedback based on direct experience. Thus, herein, experts' trust credibility (at time s) is proposed to be calculated as a normalised weighted average of their profile similarity, opinion similarity, opinion information certainty and popularity level (at time s). Let $UI_j(s)$ be the set of experts interacting with Z^j at time period s, and $UI_j(s\_k)$ be the set of experts interacting with Z^j in the kth assessment mission during time period s.

Profile Similarity. The set of characteristics/features variables that define unequivocally an expert consist of both quantitative and qualitative variables (column 1 of Table 4 of Appendix B) with domains provided in column. Thus, a similarity of profiles is obtained as the opposite of a distance between the profiles' corresponding feature vectors [49]. Similarity regarding gender, birthplace and job features is defined as a $\{0,1\}$-binary function, with value 1 outcome when experts' feature values are in the same domain category (column 2 of Table 4 of Appendix B), while similarity for the rest of features is $[0,1]$-valued with higher outcome value the closer the experts' feature values are. Therefore, if c_g^i represents the value of feature c_g $(g = 1,2,\ldots,6)$ of expert Z^i, the below profile similarity between experts is proposed:

$$Sim\_P_{ij} = \frac{1}{6}\left(\sum_{g=1,3,5}\Psi\left(c_g^i, c_g^j\right) + 3 - \sum_{g=2,6}\frac{\left|c_g^i - c_g^j\right|}{3} - \frac{|c_4^i - c_4^j|}{2}\right) \tag{1}$$

where

$$\Psi\left(c_g^i, c_g^j\right) = \begin{cases} 1 & \text{if } c_g^i - c_g^j = 0; \\ 0 & otherwise. \end{cases}$$

The profile similarity of Z^j at time period s is: $Sim\_P_j = \frac{1}{\#UI_j(s)} \sum_{i=1}^{\#UI_j(s)} Sim\_P_{ij}$.

Opinion Similarity. Different measures for different information representations have been proposed in the literature for measuring similarity of opinions [3,7]. Since the interaction and negotiation among experts is a dynamic process of exchange of opinions, which could lead to opinion modification for group consensus to be reached before the final selection process, a similarity of opinions (Sim_O_{ij}) that integrates the initial or original similarity before the consensus interaction and negotiation process ($Sim_{ij\_initial}$) and the final similarity based on the experts' opinions after consensus interaction and negotiation process (Sim_{ij_final}) may be considered more realistic and dynamic in nature than the existent similarity measures. In addition, if the change of the initial and final similarity values ($\left|Sim_{ij\_final} - Sim_{ij\_initial}\right|$) is small, i.e. when both experts' opinions have changed at a similar pace and likely in the same direction (at least when the rate of change of opinion is not small), then the dynamic similarity value should be high, otherwise it should decrease. The proposed dynamic similarity of opinions between experts is the below exponential function:

$$Sim\_O_{ij}(s\_k) = Sim_{ij\_initial}^{\left|Sim_{ij\_final} - Sim_{ij\_initial}\right|}. \tag{2}$$

The opinion similarity of Z^j at s_k is $Sim\_O_j(s\_k) = \frac{1}{\#UI_j(s\_k)} \sum_{i=1}^{\#UI_j(s\_k)} Sim\_O_{ij}(s\_k)$, while the opinion similarity of Z^j at time period s is: $Sim\_O_j(s) = \frac{1}{N_j(s)} \sum_{k=1}^{N_j(s)} Sim\_O_j(s\_k)$.

Information certainty. Let the decision matrix (opinions) of Z^j at time period s be: $Y^j(s) = [y_{pq}^j(s)]$. Entropy is a quantitative index of information uncertainty; the higher value of entropy, the more uncertainty of information. Among the existent entropy measures [8], the following is adopted herein:

$$U_j(s) = \frac{1}{m} \sum_{p=1}^{m} \left(-\frac{1}{\ln n} \sum_{q=1}^{n} x_{pq}^j(s) \ln x_{pq}^j(s) \right) \tag{3}$$

where $x_{pq}^j(s) = \frac{y_{pq}^j(s)}{\sum_{q=1}^{n} y_{pq}^j(s)}$. The information certainty of Z^j at time period s is: $C_j(s) = 1 - U_j(s)$.

Popularity level. If the trust rating of $Z^i \in UI_j(s)$ on Z^j is $r_{i\to j}(s\_k) \in [0.6, 1]$, then expert Z^i interaction with Z^j is satisfactory, i.e. $u_{i\to j}^+(s\_k) = 1$, otherwise Z^i interaction with Z^j is not satisfactory, i.e. $u_{i\to j}^+(s\_k) = 0$. Thus, the popularity level expert Z^j at time s is defined as the proportion of successful interactions with expert Z^j at time period s by other experts:

$$P_j(s) = \frac{1}{K_s} \sum_{k=1}^{K_s} u_{i\to j}^+(s\_k). \tag{4}$$

where $u_{i\to j}^+(s\_k) = \begin{cases} 1 & \text{if } r_{i\to j}(s\ k) \in [0.6, 1]; \\ 0 & otherwise.. \end{cases}$

Each expert Z^j at time period s is associated the 4-tuple $\left(C_j(s), P_j(s), Sim\_P_j, Sim\_O_j(s)\right)$. These measurements reflect the static characteristics and the dynamic behaviour of experts that influence trust credibility, which is proposed herein to be defined as the aggregated value obtained via an OWA operator [50]. Recall that the OWA operator fuses values taking into account their magnitude, which when applied to a set of n real values $(x_1, x_2, \ldots, x_n)$ returns the fused value

$$O_\Omega(x_1, x_2, \ldots, x_n) = \sum_{k=1}^{n} \omega_k x_{\sigma(k)} \tag{5}$$

where $x_{\sigma(1)} \geq x_{\sigma(2)} \geq \cdots \geq x_{\sigma(n)}$; and $\Omega = (\omega_1, \omega_2, \ldots, \omega_n)$ with

$$\omega_k = Q\left(\frac{\sum_{l=1}^{k} x_{\sigma(l)}}{\sum_{l=1}^{n} x_{\sigma(l)}}\right) - Q\left(\frac{\sum_{l=1}^{k-1} x_{\sigma(l)}}{\sum_{l=1}^{n} x_{\sigma(l)}}\right) \tag{6}$$

being $Q : [0,1] \to [0,1]$ an appropriate non-decreasing basic unit-interval monotone (BUM) membership function verifying $Q(0) = 0$, $Q(1) = 1$ used to drive the fusion process. Thus, the trust credibility of expert Z^j at time period s is

$$TC_j(s) = O_\omega\left(C_j(s), P_j(s), Sim\_P_j(s), Sim\_O_j(s)\right).$$

The higher the similarity between experts, the higher the agreement between them and, consequently, the reputation and trust evaluation between them will be higher. Thus, experts Z^j with a difference between their trust credibility and global reputation (see Section 5) above certain threshold γ_C will be regarded as a malicious expert and the expert marked as sleep mode:

$$Mode_j = \begin{cases} 0 & |Rep_j(s) - TC_j(s)| > \gamma_C \\ 1 & otherwise. \end{cases} \tag{7}$$

If the value of γ_C is too high, all experts including malicious experts will be activated, which makes trust credibility lose its significance. On the other hand, if the threshold value is too low, many honest experts may not be activated, which may see the trust evaluation system breaking down, thus against the intention of trust credibility. The level value for trust credibility threshold will be discussed in Section 7.2.1, and it is suggested to be set as 0.15. The mechanism to identify and exclude malicious experts is as follows:

Algorithm 1 Mechanism for filtering out malicious experts by trust credibility measure

Input: Profiles of the candidate experts $c_g^j(j = 1, 2, \ldots N; g = 1, 2, \ldots, 6)$, initial and final opinion similarity ($Sim_{ij\_initial}$ and $Sim_{ij\_final}(i = 1, 2, \ldots, \#UI_j(s\_k))$) between $Z^j(j = 1, 2, \ldots, N)$ and experts who interact with Z^j at $s\_k(k = 1, 2, \ldots, N_j(s))$, opinion matrix $Y^j(s)$ of Z^j, trust rating $r_{i\to j}(s\_k)(i \in UI_j(s))$ on Z^j at $s\_k(k = 1, 2, \ldots, K_s)$, global reputation $Rep_j(s)$ of Z^j at time period s, and filter threshold γ_C.
Output: The mode of candidate experts.
Step 1: Use Eq.(1) to calculate profile similarity between $Z^j(j = 1, 2, \ldots, N)$ and experts who interact with Z^j during time period s, denoted as $Sim\_P_j(s)$.
Step2: Use Eq.(2) to calculate opinion similarity between $Z^j(j = 1, 2, \ldots, N)$ and experts who interact with Z^j during time period s, denoted as $Sim\_O_j(s)$.
Step3: Use Eq.(3) to calculate opinion certainty of $Z^j(j = 1, 2, \ldots, N)$, denoted as $C_j(s)$.
Step4: Use Eq.(4) to calculate popular level of $Z^j(j = 1, 2, \ldots, N)$, denoted as $P_j(s)$.
Step5: Use Eq.(7) to determine the mode of $Z^j(j = 1, 2, \ldots, N)$. If $Mode_j = 1$, then expert Z^j can be invited to supplier evaluation; otherwise, Z^j is regarded as malicious user.

4.2. Trust feedback

Trust rating feedback for the interaction performance in the decision process is a critical aspect in the trust evaluation model. Some malicious experts can be filtered out by the above trust credibility measure, being categorised as active experts and able to interact with other active experts. Thus, the trust rating feedback among experts needs to consider: (i) the interactive experience through assessment opinions for the evaluation objects/alternatives; and (ii) the interaction quality that

should support experts to provide fair and authentic trust rating score while punishing malicious behaviours.

As aforementioned, in practice experts in the database are usually invited to participate in the decision evaluation process many times, and therefore multiple interactions between experts can happen [51, 52]. Also, each expert holds two roles: the truster role as provider of trust ratings for other experts, and the trustee role as receiver of trust ratings from other experts. As a trustee, an expert's interaction reputation is the result of aggregating the trust ratings from all recommenders; as a truster, an expert's behaviour reputation is related to the provision of constant fair trust ratings. Modelling global reputation successfully requires taking into account the interaction performance and behaviour strategy and time decay factor as well.

The direct trust rating scores from experts are the foundation for assessing trust feedback. Since active experts may involve both honest experts and malicious experts, the robustness of the trust rating feedback requires taking into consideration malicious experts. The following are important factors to consider in the feedback mechanism [49]: (i) the satisfaction level of truster's interactive experience with other experts; (ii) the number of interactions; (iii) the feedback credibility to prevent unfair feedback; and (iv) context factor, i.e. the importance of interactions between experts may be higher the higher its quality is rated.

Expert's satisfaction with previous experience/behaviour is a subjective attitude and, consequently, determines the experts' future behaviour [53]. A high proportion of satisfaction with the outcomes of previous experiences/behaviours may have positive consequences regarding future interaction intention/behaviour. Thus, honest and rational experts may not be willing to repeat interactions with experts who usually provide poor performance or behave unsatisfactory.

Based on these principles, trust rating feedback of experts, who interact towards the project assessment, is determined by their corresponding local trust scores. Based a $\{-1, 1\}$-valued trust rating $r_{j\to i} = 1$ for a satisfactory interaction and $r_{j\to i} = -1$ for an unsatisfactory interaction, the EigenTrust model [37] defines the local trust value of expert Z^j for expert Z^i as the difference between the number of satisfactory interactions ($u^+_{j\to i}$) and unsatisfactory interactions ($u^-_{j\to i}$) of expert Z^j with expert Z^i, respectively. This definition is not realistic since it provides a higher local trust value with expert Z^3 to an expert Z^1, with $u^+_{1\to 3} = 30$ and $u^-_{1\to 3} = 10$, than to an expert Z^2, with $u^+_{2\to 3} = 10$ and $u^-_{2\to 3} = 0$. Thus, an alternative definition of trust rating feedback is needed.

In this study, the $[0, 1]$-valued trust rating with semantic meaning is given in Table 1. Thus, the following satisfactory interaction ratio is proposed to compute the local trust value between experts:

$$LT_{j\to i}(s) = \frac{u^+_{j\to i}(s)}{K_s} \tag{8}$$

where $u^+_{j\to i}(s) = \sum_{k=1}^{K_s} u^+_{j\to i}(s\_k)$ and $u^+_{j\to i}(s\_k)$ as defined in (4).

Given the need for high-quality feedback from trusters, it is expected that they provide constant authentic trust rating scores; otherwise, they will be punished with dishonest behaviour. Thus, higher trust feedback is associated with truster's stable authentic trust rating score. Therefore, the trust feedback between experts, $F_{j\to i}(s)$, herein proposed is obtained via the implementation of a trust rating variance based exponential function [10] to weight the local trust value:

$$F_{j\to i}(s) = e^{-\frac{v_{j\to i}}{\sum_k v_{j\to k}}} \cdot LT_{j\to i}(s). \tag{9}$$

where $v_{j\to i} = \frac{1}{\#UI(i,j)} \sum_{l=1}^{\#UI(i,j)} (r_{j\to i}(l) - \mu_{j\to i})^2$; $\mu_{j\to i} = \frac{1}{\#UI(i,j)} \sum_{l=1}^{\#UI(i,j)} r_{j\to i}(l)$ is the average value of the trust rating score of truster Z^j for trustee Z^i; and $UI(i, j)$ is the set of interaction records between Z^i and Z^j in the time interval $[0, s]$.

The trust feedback computation in (9) plays a guiding role in trust evaluation. The lower the value of the variance $v_{j\to i}$, the greater the trust rating feedback $F_{j\to i}$ will be. The value $v_{j\to i} = 0$ happens when the trust rating score of truster Z^j for trustee Z^i is always the same when they interact, which is the case when Z^i and Z^j interact only once, in the time interval $[0, s]$. The second case happens at the initial stage of building trust relationship. Finally, the normalised trust rating feedback is computed:

$$tf_{j\to i}(s) = \begin{cases} \dfrac{max(F_{j\to i}(s), 0)}{\sum_j max(F_{j\to i}(s), 0)} & \text{if } \sum_j max(F_{j\to i}(s), 0) \neq 0 \\ 0 & otherwise. \end{cases} \tag{10}$$

5. Global reputation model

The idea of computing reputation by aggregating trust ratings from all recommenders around the trust-get-agent was suggested by Chang et al. [54]. Ureña et al. [12] developed this idea and defined global reputation considering the behaviour evolution of experts with regard to the provision by trusters of constant fair rating scores. Based on the context of trust estimation among experts who are randomly selected to participate in the GDM process, this paper calculates experts' global reputation as per the linear combination of the below two reputation aspects of experts, as illustrated in Fig. 3 and formulated in (11):

$$Rep_i(s) = \omega_R IR_i(s) + (1 - \omega_R) BR_i(s), \quad \omega_R \in [0, 1]. \tag{11}$$

(1) interaction reputation of an expert as trustee, $IR_i(s)$; this aims to capture trustees' trust rating scores of interaction with other experts; it depends on an expert's history of interactions with all the experts in the database.
(2) behaviour reputation of an expert as truster, $BR_i(s)$; this aims to capture trusters' performance when providing trust ratings; it depends on the evolution of the given trust ratings and the activity level of the truster.

The range of an expert's reputation is set as $[0, 1]$. Since at the initial stage of the evaluation process there is no interaction among experts, there is neither information related to the expert's behaviour nor trust rating scores; taking into consideration the professional qualifications and experience of expert, an initial global reputation value $Rep_i(0) = 0.6$ is thus provided to each expert in the database.

5.1. Interaction reputation

While interaction reputation is based on the aggregation of trust rating feedback from other experts (Section 4.2), the reliability of each expert node is crucial to motivate experts to provide fair trust ratings for other experts and, consequently, to guarantee the effectiveness of reputation. As described in Section 4.1, trust credibility is developed in terms of the performance of the expert itself (integrity) other than trust rating, and filters out the malicious trusters (Section 3.2). The reliability of trust rating comes mainly from rating quality and the expected trust rating. Then, assigning weight to rating providers (i.e., experts as trusters) according to their reliability performance will connect the trust rating scores with the impact on the trustees' reputation. Fig. 4 illustrates this scenario.

Given the context of trust rating that contributes to the interaction reputation of expert $Z^j, (j = 1, 2, \ldots)$, the interaction reputation considers the critical factors related to the rating score to measure either the honesty or influence level of a trust rating. Thus, the effect of the historical interaction and recent behaviour of other experts on the interaction reputation of trustee is modelled along the following lines.

The effect of interaction quality. In some cases, a malicious truster may build a good reputation initially by providing fair and authentic trust rating scores. However, they will then destroy their reputation by providing unfair bad ratings to other experts [55]. Thus, reputation measurement should consider interaction quality so that the expert provides a constant fair trust rating. The

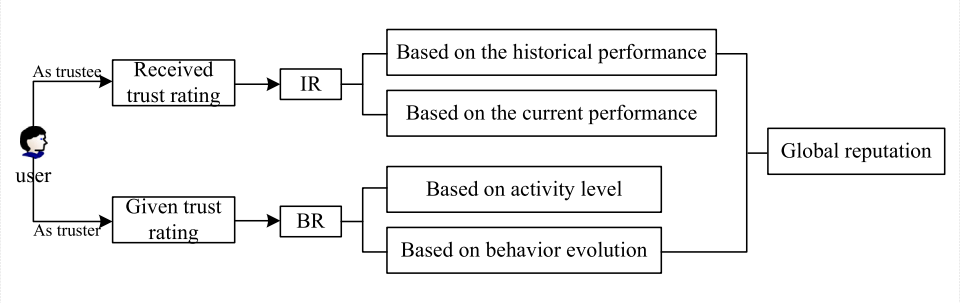

Fig. 3. Reputation main components.

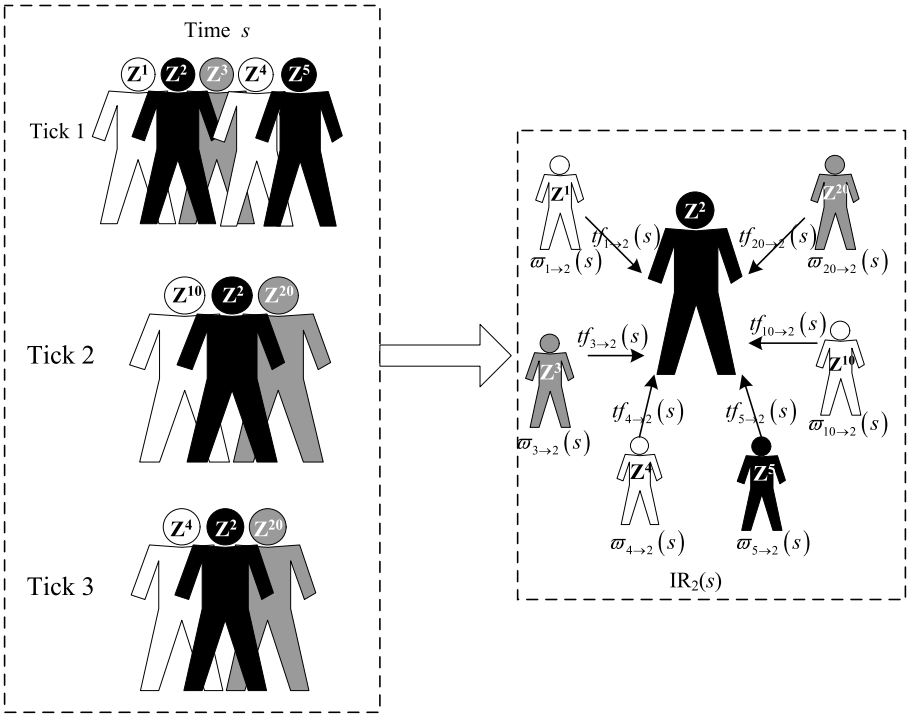

Fig. 4. The visualisation of interaction reputation of the expert in period s.

detection of a fair rating depends on the gap between the received trust rating score and his/her previous reputation. Thus, an expert's reputation increases if, after each project assessment process, the expert receives a trust rating that is close to his/her previous reputation. That is if trusters provide fair trust rating scores, there would be a positive impact on their influence level, while the given unfair trust ratings would decrease their rating weights. Thus, the truster-reputation $\varpi_{truster}(j \to i, s)$ is proposed to be updated from $\varpi_{truster}(j \to i, s-1)$ as follows:

$$\varpi_{truster}(j \to i, s) = \varpi_{truster}(j \to i, s-1) \cdot \left(1 - \frac{\left| IR_i(s-1) - tf_{j \to i}(s) \right|}{\#UI_j(s)}\right) \tag{12}$$

where $UI_j(s)$ is the set of experts who interacting with Z^j during the period $[0, s]$; and initial assignment weight $\varpi_{truster}(j \to i, 0) = 1$ and initial interaction reputation $IR_i(0) = 0.6$ (see above initial value of global reputation).

The expected utility of trust feedback. A trust rating score for an expert is influenced by the expert's justification of the character and abilities of other experts. Based on the expected utility theory [56], an expert's reputation expectation may increase as the expert's received trust feedback increases. Moreover, a significant difference between the trust feedback and the average rating score can heighten the possibility that the provider is fraudulent. Thus, the expected utility of trust feedback models the partial influence of interaction and average rating scores on the interaction reputation of Z^i and Z^j:

$$\varpi_E(j \to i, s) = e^{-\left| \frac{tf_{j \to i}(s) - \overline{tf}_{j \to i(s)}}{\overline{tf}_{j \to i}(s)} \right|} \tag{13}$$

where $\overline{tf}_{j \to i}(s) = \frac{1}{\#UI_i(s)} \sum_{j \in UI_i(s)} tf_{j \to i}(s)$ is the average received trust feedback on trustee Z^i during the period $[0, s]$.

Notice that $\varpi_{truster}(j \to i, s)$ is a weight coefficient based on the (previous) trustee reputation of expert Z^i at period $s-1$, while $\varpi_E(j \to i, s)$ is a weight coefficient based on the trust feedback received by the expert from other experts at current time period s. The interaction reputation is therefore associated with the two intertwined influence factors: the rating quality compared with historical performance and the expected rating score compared with the current received rating [10]. Thus, the proposed interaction reputation of a trustee is to be computed as the below weighted average of the trust feedback the trustee receives (at

time s):

$$IR_i(s) = \frac{1}{\#UI_i(s)} \sum_{j \in UI_i(s)} \varpi_{j \to i}(s) \cdot tf_{j \to i}(s), \tag{14}$$

$$\varpi_{j \to i}(s) = \frac{2\varpi_{truster}(j \to i, s) \cdot \varpi_E(j \to i, s)}{\varpi_{truster}(j \to i, s) + \varpi_E(j \to i, s)}. \tag{15}$$

5.2. Behaviour evolution

The interaction reputation of an expert refers to the global trust rating feedback based on the received trust rating feedback as a trustee. The behaviour reputation involves the activity level of experts and the difference between the current trust rating feedback and the previous global reputation value, and it aims at measuring the change of behaviour.

The more project assessments an expert is engaged in, the more experienced the expert becomes. The concept of activity level proposed herein aims to reflect the satisfaction experience of the interactions that experts have participated in. Thus, the activity level of an expert Z^i at time period s is proposed to be measured using the ratio of satisfactory interactions the expert was involved in such period of time

$$A_i(s) = \frac{1}{K_s} \sum_{k=1}^{K_s} \frac{u_i^+(s\_k)}{N_i(k)}, \tag{16}$$

where K_s is the number of assessment missions that expert Z^i was invited to participate at time period s; $u_i^+(s\_k) = \sum_{j=1}^{N_i(k)} u_{i \to j}^+(s\_k)$; and $N_i(k)$ is the number of experts in the $k-$th assessment mission where Z^i was involved and interacted with.

The satisfaction with the historical interactions is critical in encouraging other experts in the system to behave well at all times. The activity level is expected to provide an incentive for the database expert to emphasise behaviour history. Numerous satisfactory interactions performed by expert Z^i may improve that expert's activity level. In case like that, the selected experts will have to behave honestly during the initial period of time to build up a positive reputation before starting the self-serving attack. In any case, the behaviour reputation is designed to encourage long-term good behaviour by promoting experts to provide authentic trust ratings and punishing experts' behaviour changes that may indicate they are aiming to promote their own, not the collective, strategic interests. Thus, the effect of the historical and recent behaviour of an expert Z^i is to be reflected in that expert's behaviour reputation as follows: a sharp increase or decrease between the previous global reputation value and the current trust rating feedback value would be an indicator of malicious behaviour, and such expert's behaviour reputation will be significantly affected; when an expert's trust rating remains relatively stable, the difference between the previous global reputation value and the current trust rating feedback value will be close to 0, and such expert's behaviour reputation will not be significantly affected.

The above can be modelled by defining expert's $BR_i(s)$ value as follows:

$$BR_i(s) = A_i(s) - \frac{1}{\#UI_i} \sum_{j \in UI_i(s)} \left| tf_{i \to j}(s) - Rep_i(s-1) \right|. \tag{17}$$

As with initial interaction reputation, the initial behaviour reputation value $BR_i(0) = 0.6$ is used.

Due to the dynamic characteristics of trust relationship, the reputation model should emphasise the impact of timeliness relevance. Numerous researches address this issue by introducing a time decay factor [57,58]. The Ebbinghaus' forgetting curve has demonstrated that the forgetting process of human begins immediately after learning with a gradual and non-linear trend. As per the above decay model, if an expert Z^i does not participate in any assessment missions after period s, then its corresponding reputation value is updated and reduced at those period time using a positive decay factor value ϕ and the corresponding time elapsed since the expert's last assessment and interaction participation:

$$Rep_i(t) = \frac{1}{1 + \phi \cdot (t - s)} \cdot Rep_i(s), \quad t > s. \tag{18}$$

Table 2
Normalised trust rating feedback and identity level of recommenders.

Trust degree	–	[0,0.6)	[0.6,0.8)	[0.8,0.9)	[0.9,1]
Identity level	V_0	V_1	V_2	V_3	V_4

6. Comprehensive trust evaluation

In the previous section, the trust evaluation computation is based on direct interactions. However, the sparsity of the trust network may imply the non-existence of a direct interaction experience between some of the experts, say Z^j and Z^i. These cases are addressed next with an approach based on the information obtained using indirect experience from other participants, who are referred to as witnesses/recommenders.

6.1. Recommend trust

Recommend trust from Z^j and Z^i is computed using the trust rating scores of each witness/recommender, Z^h, who has previously interacted with the trustee Z^i. These indirect experts are obtained by the trust manager by querying the database. Since not all feedback from experts is honest, the trust credibility test described in Section 4.1 is applied to detect malicious experts, who are marked as sleep mode. Thus, only feedback from experts marked as active mode is treated as witness information by the trust manager.

For the collected witness information, determining the identity of the witness/recommender is a priority. This obviously depends on the interaction history and the trust degree between the truster Z^j and the witness/recommender Z^h. There are two types of interaction situations, one without interaction, and the other with different trust ratings on recommenders. Based on Table 1, the witness evidence will could not be trusted if the trust rating on recommender is lower than 0.6; otherwise, the witness evidence that deserves trust corresponds to different levels. Thus, an algorithm for trust authorisation levels of the witness/recommender is designed to divide witness/recommender into different levels, with the following steps:

(1) The initialisation step is used to check the interaction records of truster Z^j. If he has no interaction with the witness/recommender Z^h, then Z^h is classified as a stranger and denoted as V_0.
(2) The assignment step is used to calculate the normalised trust rating feedback $tf_{j \to h}$ of truster Z^j to each recommender Z^h. The trust semantics of Table 1 is then applied to normalised trust rating feedback to map the recommender Z^h to the identity levels of Table 2.

Notice that when $tf_{j \to h} \in [0, 0.6)$, the recommender is given the distrust level V_1; when $tf_{j \to h} \in [0.6, 0.8)$, the recommender is given the average trust level V_2; when $tf_{j \to h} \in [0.8, 0.9)$, the recommender is given the fairly trust level V_3; when $tf_{j \to h} \in [0.9, 1]$, the recommender is given the complete trust level V_4. The higher the level is, the more likely the witness information is to be adopted. Consequently, the more weight is given to a witness/recommender the higher its label is. Let $\lambda_g = \frac{\#V_g}{\sum_{i=0}^{4} \#V_i}$ be the weight associated to the $\#V_g$ recommenders with lable V_g $(g = 0, 1, \ldots, 4)$. Then, the following recommend trust at period

s is proposed

$$tr_{j\to i}(s) = \lambda_0 \frac{\sum_{h_0=1}^{\#V_0}\sum_{d=1}^{s-1} Rep_{h_0}(d)\cdot tf_{h_0\to i}(d)}{\sum_{h_0=1}^{\#V_0}\sum_{d=1}^{s-1} Rep_{h_0}(d)} + \lambda_1 \frac{\sum_{h_1=1}^{\#V_1}\sum_{d=1}^{s-1} Rep_{h_1}(d)\cdot tf_{h_1\to i}(d)}{\sum_{h_1=1}^{\#V_1}\sum_{d=1}^{s-1} Rep_{h_1}(d)} + \lambda_2 \frac{\sum_{h_2=1}^{\#V_2}\sum_{d=1}^{s-1} Rep_{h_2}(d)\cdot tf_{h_2\to i}(d)}{\sum_{h_2=1}^{\#V_2}\sum_{d=1}^{s-1} Rep_{h_2}(d)} + \lambda_3 \frac{\sum_{h_3=1}^{\#V_3}\sum_{d=1}^{s-1} Rep_{h_3}(d)\cdot tf_{h_3\to i}(d)}{\sum_{h_3=1}^{\#V_3}\sum_{d=1}^{s-1} Rep_{h_3}(d)} + \lambda_4 \frac{\sum_{h_4=1}^{\#V_4}\sum_{d=1}^{s-1} Rep_{h_4}(d)\cdot tf_{h_4\to i}(d)}{\sum_{h_1=4}^{\#V_4}\sum_{d=1}^{s-1} Rep_{h_4}(d)} \tag{19}$$

6.2. Comprehensive trust

During the GDM process, experts may fail to reach an agreement at the initial stage and the consensus reaching process needs to be carried out [3–8]. When active experts are chosen to participate in assessing, each expert conducts trust evaluation on other experts in the same review panel according to their interaction process performance. At each period s, experts' comprehensive trust information, see Fig. 5, is computed as a weighted average of their corresponding recommend trust (indirect trust) and trust rating feedback (direct trust)

$$T_{i\to j}(s) = \pi_{i\to j}(s)\cdot tf_{i\to j}(s) + \left(1-\pi_{i\to j}(s)\right)\cdot tr_{i\to j}(s). \tag{20}$$

Determining the value of the weight factor $\pi_{i\to j}(s)$ is a crucial issue in this model, and this can be done based on subjective or objective judgments or a combination of both types of judgments. In any case, the dynamic nature of the interaction between experts means that assignment of the weight for direct trust and indirect trust should also be dynamic. Generally, experts put more trust in their own direct interaction experience than in third-party recommendations. That is, a higher weight should be allocated to direct trust feedback than to recommend trust. Notice that when Z^i has no interactions with expert Z^j at period s, then there is only recommend trust at this period, and therefore it would be $T_{i\to j}(s) = tr_{i\to j}(s)$. This can be achieved with the above when $\pi_{i\to j}(s) = 0.$. An example of functional weight factor that fits this case is $\pi_{i\to j}(s) = h(\#UI_{i\to j}(s))$, where $\#UI_{i\to j}(s)$ denotes the number of interactions of expert Z^i with expert Z^j at period s. In particular, herein we are proposing

$$\pi_{i\to j}(s) = 1 - \theta^{\#UI_{i\to j(s)}}, \tag{21}$$

where $\theta \in (0, 0.5]$ so that, when interactions of expert Z^i with expert Z^j at period s do exist, a higher weight is allocated to direct trust feedback than to recommend trust. The value of $\theta \in (0, 0.5]$ can be determined by each expert to represent how "experts value their own interaction experience", with values closer to zero indicating a higher valuation of their own interaction experience.

7. Experimental results and discussion

There are mainly two approaches to evaluate the effectiveness of the proposed trust model in trust management. One is based on simulation, the other is based on real-world data sets. While some datasets on trust assessment are available (such as Epinions and Extended Epinions datasets [59]), it is often difficult to find suitable real-world data to assess the effectiveness of various trust models under different deceptive environments. Therefore, most of the existing trust models are evaluated using simulation or synthetic data. The agent reputation and trust testing platform proposed in [60] is one of the most popular trust model simulation testing platforms currently used in trust research. However, this testbed is applicable to service providers and clients that are interacting with each other although only the trust information of the customer towards the service providers is available. The trust evaluation framework in this study is based on trust feedback from experts as trusters and trustees, and the profile information of experts is also included. Therefore, customised simulation environments are designed to evaluate the performance of the proposed reputation and trust model.

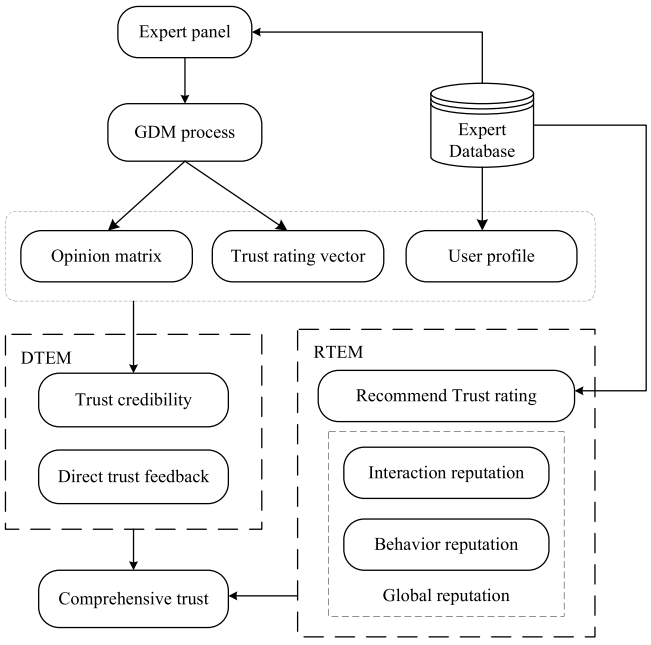

Fig. 5. Trust computation model.

7.1. Simulation environment and experimental setup

The runtime environment to simulate a dynamic interaction scenario with a cold-start system is constructed based on the following settings:

Simulation setup: We generated an expert system with 50 experts who interacted with each other during a year, with 15–25 rounds of review missions conducted every month, with about 3,000 records. The cold start of the simulation is implemented with a default global reputation score of 0.6 assigned to each expert. The experts' profiles are set based on the required fields. It is assumed that an expert has no prior interaction experience at the start of the simulation ($s = 0.$). Therefore, experts are randomly selected to form an expert group for the assessment mission. Each expert can engage in 3 activities (programme assessment, trust evaluation and recommendation) and play 3 different roles (truster, trustee, and recommender). Administrator calculates the reputation values of the experts in the database who participate in assessing every other month. This value will be applied in subsequent steps.

Each expert can show different satisfaction with interaction quality (such as rating) according to their own satisfaction standards. At the beginning of the simulations, we assume that the subjective trust rating r follows a normal distribution $r \sim N(0.6, 0.01)$. After each interaction, the trust ratings given by the expert fluctuate based on the last trust ratings, indicating the error caused by the environment and subjective perception. In other words, each expert takes the trust score of the last interaction as benchmark, and the value fluctuates ± 0.1. At this point, the initialisation of trust ratings between all experts is completed.

In the simulations, we assume that there are two different types of experts: (1) honest experts, who sometimes provide inaccurate ratings but fair behaviour; (2) malicious experts, who are detected to be deceptive behaviour. In an expert database management system, each expert is assigned a unique and stable ID through a policy mechanism, which can avoid white-washing. Contrary to the consumer reviews websites, the trust evaluations from experts are relatively private, thus experts have no incentive to provide dishonest ratings because of self-promoting, slandering or bad-mouthing. For this expert database, there are two types of malicious attacks: traitor and collusion, as described in Section 3.2. Regarding performance, the trust ratings from traitors are higher than the authentic rating in the early stages while they are lower than the authentic rating during the late stages; the trust ratings in $[0.8, 1]$ are used for the collusive members while the trust ratings in $[0, 0.6)$ are for experts outside the collusive group.

Evaluation metrics: The type of metrics used depends on the object of the reputation and trust model. The purpose of this study is to establish the trust relationship between experts and provide support for experts in the decision process. A good reputation model in the application process should prefer honest experts with high reputations over malicious experts. In the simulation, it is shown that when honest experts high on the reputation list are selected in the repeated interaction process, the better the reputation model is. Meanwhile, when the comprehensive trust degree between experts is closer to the authentic trust feedback during the process of interaction, the higher accuracy of the trust model is. Therefore, the success of the trust model based on reputation depends on its accuracy in predicting future trust relationships. Based on the above analysis, the precision degree Pre and similarity degree Sim are introduced to describe the performance of the reputation and trust model.

Precision degree. Pre reflects the success of reputation model in resisting malicious attacks through the ratio of active top-ranked honest users:

$$Pre(s) = \frac{\#(R^{+}(s) \cap R(s))}{\#(R^{+}(s) \cup R^{-}(s))}, \tag{22}$$

where $R(s)$ is the set of experts at period s throughout the entire space of active experts; $R^{+}(s)$ and $R^{-}(s)$ are the set of n top-ranked honest experts and malicious expert (by reputation value), respectively.

Similarity degree. Sim presents the divergence between the comprehensive trust values at $s-1$ and the actual trust rating feedback values at s:

$$Sim(s) = 1 - \frac{1}{\#E(s)} \cdot \frac{1}{\#IR_i(s)} \sum_{i \in E(s)} \sum_{j \in IR_i(s)} \left| T_{i \to j}(s-1) - tf_{i \to j}(s) \right|, \quad (s \geq 2), \tag{23}$$

where $E(s)$ is the set of experts who participate in the GDM process at period s, and $IR_i(s)$ is the set of experts interacting with Z^i at the period s.

7.2. Experimental results and analysis

In this paper, we introduce the reputation-based trust model and investigate trust quantification in the consensus process of GDM problem. It learns from the trust mechanism of the relationship between human societies, evaluates peer's trust via direct trust feedback and recommend trust.

This section verifies the robustness and anti-attack ability of the reputation model, and the validity of the reputation-based trust model in estimating the trust degree between experts. First, the deceptive environments in the reputation model and trust model are described: (1) *deceptive environments with intermittent ratings:* traitors change their behaviour intermittently to damage the reputation system in the process of trust evaluation; in such setting, trusters attempt an attack in the form of high-low-high-low rating; (2) *deceptive environments with collusion:* attackers might form a small clique by colluding and leveraging their relationship to destroy the reputation and trust model; in this simulation, the size of the collusive group is equal to the total number of malicious experts, and they provide high trust ratings for collusive members and for experts outside the collusive group low trust ratings.

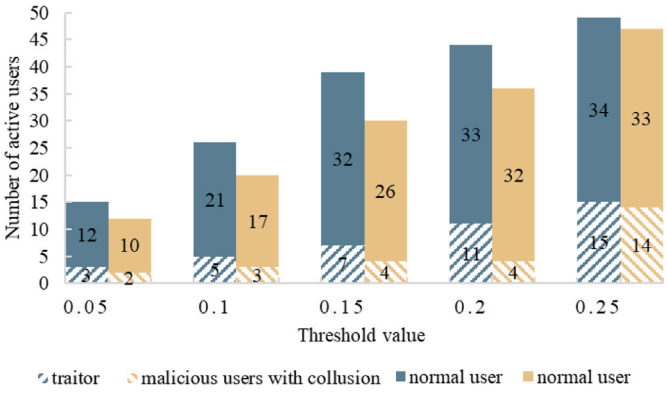

Fig. 6. Active experts with different threshold values.

7.2.1. The sensitivity of trust credibility

Experts filtered as active mode have access to participate in the assessing process; the chances of selecting each expert as active not only relate to the value of their reputation but also the value of their trust credibility, so even a low-reputation expert has a chance to be selected as active. The following analyses the effect of trust credibility on the expert database system with different threshold values. The trust credibility is designed to filter out malicious experts. It is assumed that 30% of the 50 experts (15) in the expert database are malicious experts (traitor or collusion). Then, the number of active experts under different threshold values is listed in Fig. 6.

On the one hand, it is obvious that the number of active experts increases as the threshold value γ_C increases: when $\gamma_C = 0.25$ nearly all of the experts are classified as active while less than half of the experts are classified as active when $\gamma_C = 0.05$. To some extent, some of the 15 malicious experts are identified by the trust credibility screening and filtered out as sleep mode, with the number being higher the lower the value of the threshold γ_C is. Thus, the effectiveness of trust credibility, especially for the collusion attack, in identifying malicious experts increases as the value of the threshold γ_C decreases. The simulation shows that the number of malicious experts with collusion classed as active has little variation when γ_C ranges from 0.05 to 0.2, while the effect of the trust credibility measure is less evident when filtering traitor experts. Thus, the reputation-based trust evaluation described in Section 5 is needed to improve the robustness and anti-attack ability of the proposed model, and its effectiveness will be discussed in the next two subsections. On the other hand, Fig. 6 shows that active experts are few in number when $\gamma_C = 0.05$ and $\gamma_C = 0.1$, which is inefficient since expert resource utilisation is wasted. Given this, it is unsuitable for γ_C to be set very low in value like 0.05 or 0.1. Meanwhile, the trust credibility measure plays little or no role in filtering malicious experts when $\gamma_C = 0.25$. In summary, the value $\gamma_C = 0.15$ is, of all the simulated values, the one at which the trust credibility measure performs best in balancing the proportion of all users identified as active experts with the number of users filtered as malicious experts.

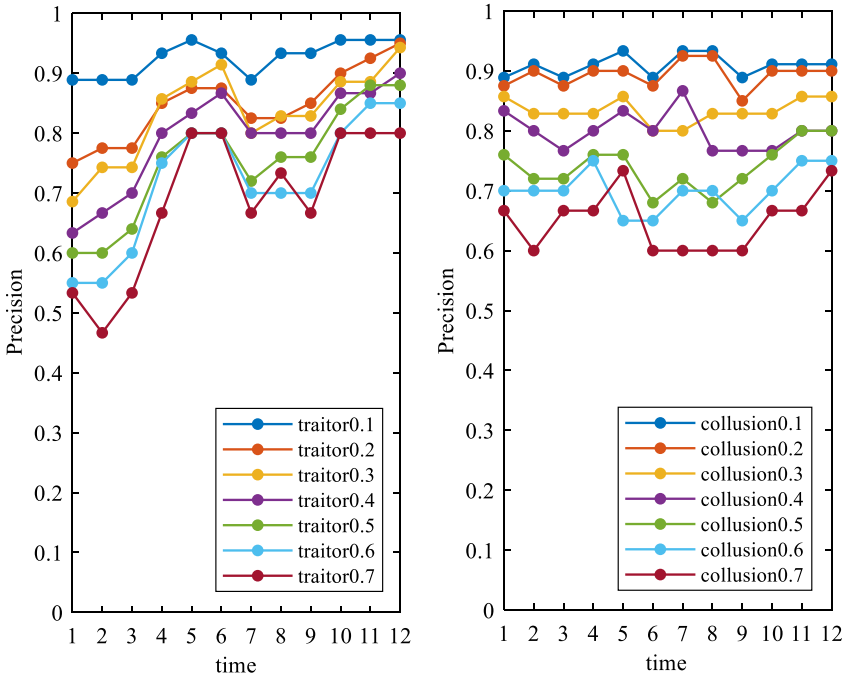

Fig. 7. The precision degrees of the reputation model in deceptive environments.

7.2.2. Discussion of reputation model

The effectiveness of the reputation model lies in the quality of the model rather than the trust ratings. This model aims to estimate the reputation of experts and regularise their behaviour in the evaluation process. Thus, the reputation of the honest expert, whose trust ratings are consistent and stable, is improved gradually while the reputation of the malicious expert is gradually decreased. The simulation of interactions between experts was run for one year and the variation of the precision degree, with a proportion of malicious experts (traitor or collusion) ranging from 0.1 to 0.7, are shown in Fig. 7. In general, the precision degree decreases when the proportion of malicious experts increases. It is noticeable that the precision value of the reputation model with traitor behaviour is associated with time, i.e., the periodic change due to intermittent ratings. When the ratings from malicious experts drop dramatically at times 4 and 10, it brings a low reputation for traitors and a higher precision level for the reputation model; when the malicious experts increase unfair trust ratings at time 7, there is a significant decrease in precision value. Nonetheless, the precision level improved with time, which is attributed to the identification and filtering out of malicious experts by the behaviour reputation and trust credibility.

No precision fluctuation regularity of the reputation model with collusion is observed though, which is generally driven by the expert's group membership information changes in the GDM situation. It should be noted that the precision level is generally higher when the proportion of malicious experts is less than 0.5, which is also observed in the average precision values illustrated in Fig. 8. This result can be attributed to the following reasons: (1) the unfair rating records under the attack of collusion might be lower than the interaction records from traitors because collusion is a group behaviour and will be triggered until collusive members are assigned to the same group; (2) the trust credibility is effective in filtering out unfair ratings if the number of malicious experts is lower than half of the total experts in the database; this filtering method becomes invalid when there are too many malicious experts; (3) the interaction reputation can reduce unfair rating's impacts on the model, thereby limiting the boosting of the reputation of malicious experts as a result of the collusive behaviours. In a real world scenario, it is unreasonable for an expert database to have more than half of them in collusion. In such setting,

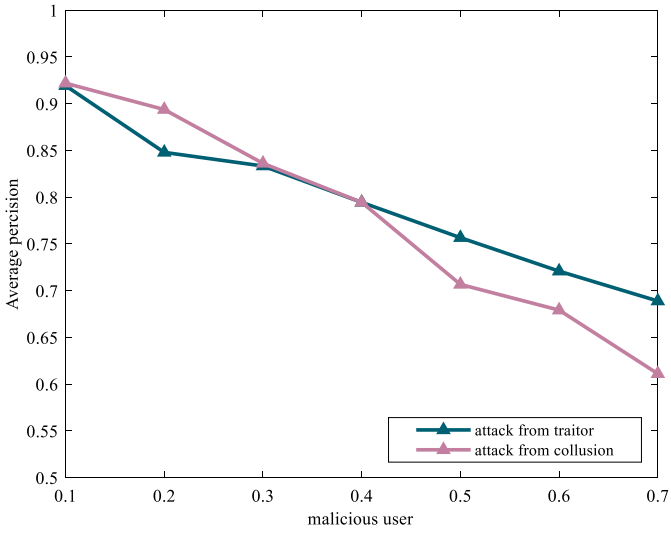

Fig. 8. Average precision degrees of the reputation model in deceptive environments.

the interactions between honest experts are restricted. To avoid such a scenario, new experts need to be invited into the expert database if the available active experts are less than half of the total experts.

7.2.3. Discussion of reputation-based trust model

The performance of the proposed trust model in the estimation of trust relationship between experts in the database increases the closer the comprehensive trust degree between truster and trustee during the process of interaction is to the true trust evaluation given by experts in the next period of time. The similarity degrees between experts in the one-year simulated interactions between experts, with a proportion of malicious experts (traitor or collusion) ranging from 0.1 to 0.7, are shown in Fig. 9. The similarity degrees decrease gradually as the proportion of malicious experts increases while they increase over time. Sensitivity to the proportion of malicious experts by the similarity degrees is higher under the attack of traitors than the collusive experts.

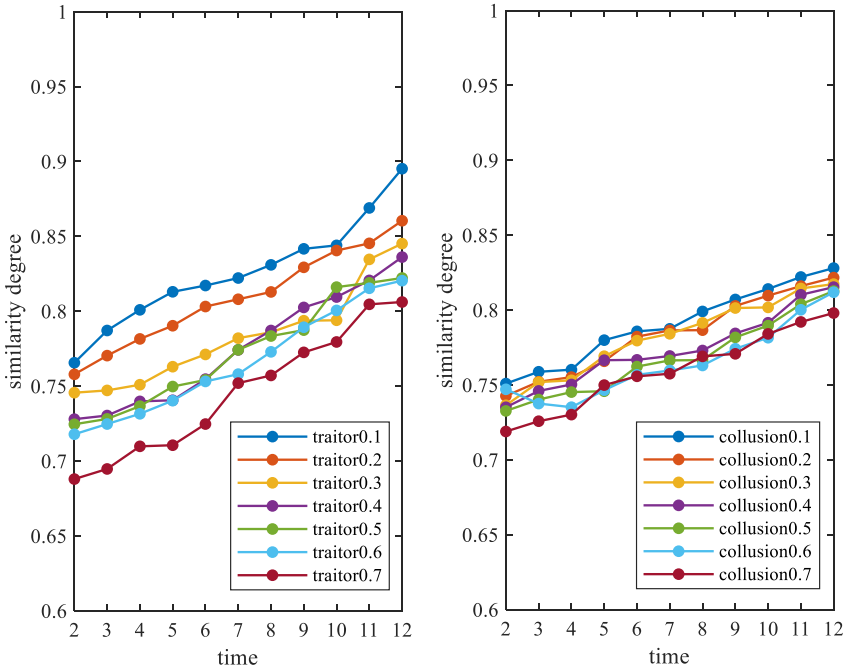

Fig. 9. The similarity degrees of the trust model in deceptive environments.

There are several explanations for this phenomenon: (1) traitors provide intermittent dishonest ratings, which is individual behaviour; an increase in the proportion of traitors indicates that the reputation of more honest experts will be destroyed; in contrast, collusion is a group activity, and while these malicious experts might not be invited into the same assessment mission and still provide fair ratings for the honest experts; (2) intermittent behaviour is much easier to be identified than collusion; despite being protected by the setting of the proposed behaviour reputation and interaction reputation, the similarity degree of trust estimation is still affected by the attack from traitors to some extent. On balance, the similarity degrees of the trust model under the considered attacks go above 0.8, which is considered as satisfying the requirement of accuracy. This shows that increasing the direct interactions between experts will raise the accuracy level of the trust model.

7.3. Discussion: Advantages and limitations

In this section, we point out some of the advantages and limitations of the reputation-based trust model in GDM.

7.3.1. Advantages

To date, different trust models have been used for solving GDM problems. This paper developed a comprehensive trust model from direct trust feedback and reputation-based recommend trust in GDM and detected malicious users based on trust credibility measure. This section compares the proposed reputation-based trust model with some existing trust models [3–8,10,12,33–35]. In particular, we identified the following highlighted features of the reputation-based trust model when compared with existing trust models:

(1) Trust ratings. The trust ratings from experts are key elements in the GDM process. However, the trust ratings have long been supposed to be honest and fair [3–7]. In this study, the malicious attacks that might exist in experts' interactions with other participants, such as dishonest rating and collusion, is considered to improve the performance of trust model. As we analysed in Section 7.1, there may exist dishonest ratings or unfair ratings due to collusion among some experts. The proposed trust model could efficiently handle the dishonest rating and collusion when present in experts' trust ratings in the dynamic interaction during GDM process compared with other models for building trust relationships [5,8].

(2) Methods used to filter out malicious users. In [33], the Bayesian reputation system is applied only to that most of users would provide honest ratings. The reputation model in [10,12,35] can reduce the negative effects of malicious behaviours, but a much better option is to prevent malicious users from participating directly. In [34], Teacy et al. applied the personal observations of users regarding trusters to detect and filter out deceptive ratings. In this study, we developed an approach based on trust credibility measure to filter out malicious experts by judging whether the performances of experts beyond trust assessment match their reputation. To the best of our knowledge, this is the first study that detects malicious experts from experts' profiles and opinion similarity, the accuracy of experts' opinions, and the popularity level of each expert.

(3) Reputation model. Compared with the reputation model presented in [35], the proposed reputation model was constructed from several aspects including interaction process and behaviour evolution, which enhances the source of reputation evidence in the trust implementation process. Compared with the reputation model developed in [10,12], the trust feedback in our proposal can provide high robustness to malicious attacks and a guide to trust evaluation. Furthermore, the time decay factor is considered into the proposed reputation model to reduce the weight of historical trust feedbacks.

(4) Dynamic comprehensive trust model. The trust recommendation on trustee may vary widely depending on the identity level of recommender, and the trust feedbacks of experts as trusters will evolve in the implementation of trust evaluation model; however, this issue is not discussed in [3–5,7,12]. By taking into account the direct trust feedback and the recommend trust, this study developed a comprehensive trust model for the interactions among experts during GDM process. Moreover, a detailed simulation is provided in Section 7 to complement the main features/ characteristics of the proposed trust model. The above comparison shows that this study constructs a novel dynamic

Table 3
Used parameters.

Notions	Illustration
$Z = \{Z^1, Z^2, \ldots, Z^N\}$	A set of experts
$r_{j\to i}(s\_k)$	The trust rating of Z^j on Z^i in the kth assessment mission in the period s
$\mu_{j\to i}$	The average value of trust rating score of truster Z^j for trustee Z^i
$\nu_{j\to i}$	The variance value of trust rating score of truster Z^j for trustee Z^i
$C_j(s)$	The trust credibility of Z^j in the period s
γ_C	The threshold of trust credibility
$LT_{j\to i}(s)$	The local trust value of Z^j on Z^i in the period s
$F_{j\to i}(s)$	The trust feedback value of Z^j on Z^i in the period s
$tf_{j\to i}(s)$	The normalised trust feedback value of Z^j on Z^i in the period s
$tr_{j\to i}(s)$	The recommend trust value of Z^j on Z^i in the period s
$T_{j\to i}(s)$	The comprehensive trust value of Z^j on Z^i in the period s
λ_g	The weight of recommender cluster
$IR_i(s)$	The interaction reputation value of Z^i in the period s
$BR_i(s)$	The behaviour reputation value of Z^i in the period s
$Rep_i(s)$	The global reputation value of Z^i in the period s
$\varpi_{j\to i}(s)$	The weight assignment when Z^j provides trust rating on Z^i in the period s
$UI(i,j)$	The set of interaction records between Z^i and Z^j in the time interval $[0, s]$
$UI_j(s)$	The set of experts who interacting with Z^j in the time interval $[0, s]$
$UI_j(s\_k)$	The set of experts who interacting with Z^i in the kth assessment mission during time period s
K_s	The number of assessment missions in the period s
$N_i(s)$	The number of assessment missions that Z^i participate in the period s
$N_i(k)$	The number of experts in the kth assessment mission that Z^i was involved

comprehensive trust model that considers some practical features, which is capable of dealing with malicious behaviours and trust evolution issues during the interaction process.

7.3.2. Limitations

We find the following limitations to the study, which require future research efforts.

(1) In general, different experts may provide different forms of trust ratings due to individual experience and prior knowledge. This study develops a reputation-based trust model from an interdisciplinary perspective by integrating direct trust feedback and recommend trust in the context of GDM. To the best of our knowledge, it is an open problem when modelling personalised individual semantics and consensus [24]. Thus, we argue that it will be worthwhile to design some methods to extend our trust model with other trust information representations.
(2) In our proposal, trust and reputation systems are assumed to, as other informatics systems, suffer from vulnerability to the most common attacks, which fail to take other factors in the actual GDM process, such as false-consensus effect. Therefore, it would be very interesting to investigate the trust system in a dynamic complex malicious environment. Further research on characteristics of malicious behaviours and solutions is needed under GDM process.
(3) The trust-based application in our proposal is relatively simple and lacks large-scale application demonstration projects. In practice, the proposed trust model may be difficult to support the reliability of trust quantitative evaluation of complex application systems. For instance, it may be most likely that experts belong to several different social communities due to their diverse interests, research fields, and families. This issue is called overlapping community and has been investigated in social network GDM [26]. However, the trust-based community structure is not considered in our proposal. Therefore, it will be interesting in future research to design an approach to manage the impact of trust structure on the consensus process.

8. Conclusion

Focusing on the trust formation among experts in the context of GDM process, this study proposed a reputation-based trust model that takes into account the direct trust from the interaction between experts and the recommendation information from indirect experts.

We first analysed and defined the trust credibility measure from the similarity of profile and opinion, the information accuracy and popularity level, and defined the direct trust rating feedback based on the experts' interaction quality. In order to assign weights for recommenders, a reputation model was developed to investigate experts' behaviour performance. Next, we employed dynamic weight factor and the interaction principle to aggregate the direct trust rating feedback and the recommend trust to derive comprehensive trust. The trust management system and simulation in the assessment process have demonstrated that the trust and reputation model is effective even in the presence of malicious experts.

The proposed reputation and trust models were developed to simulate GDM scenarios. However, there are some limitations that require to be investigated in the future. For example, trust indicators related to experts require further study. Although the trust credibility measure can filter out some malicious experts when constructing the direct trust model, there are still some dishonest experts who meet the threshold level, and can participate in the evaluation process. This requires further exploration to increase the filtering efficiency.

CRediT authorship contribution statement

Xinli You: Conceptualization, Methodology, Investigation, Validation, Software, Writing – original draft. **Fujun Hou:** Methodology, Formal analysis, Validation, Supervision. **Francisco Chiclana:** Supervision, Validation, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors are unable or have chosen not to specify which data has been used.

Appendix A. List of parameters and their descriptions

See Table 3.

Table 4
Index interval.

Index	Classification interval and representative values
Gender (c_1)	Female (0)
	Male (1)
Age (c_2)	[20,30) (2)
	[30,40) (3)
	[40,50) (4)
	[50,60) (5)
Birthplace (c_3)	Beijing (1)
	Hebei (2)
	Northeast region (3)
	Henan (4)
	Shandong (5)
	Anhui (6)
	Hubei (7)
	Sichuan (8)
	Shananxi (9)
	Guizhou (10)
	Yunnan (11)
	Gansu (12)
	Tianjin (13)
	Jiangsu (14)
	Other provinces (15)
Education (c_4)	Bachelor (0)
	Master (1)
	Doctor (2)
Job (c_5)	Public official (1)
	University and Institute Researcher (2)
	State-owned Enterprises employee (3)
	Private enterprise employee (4)
Title (c_6)	Junior (1)
	Intermediate (2)
	Associate senior (3)
	Senior (4)

Appendix B. Profile features modelling

See Table 4.

References

[1] V. Tundjungsari, J.E. Istiyanto, E. Winarko, R. Wardoyo, 2010 International Conference on Distributed Frameworks for Multimedia Applications, 2010, pp. 1–7.

[2] R. Urena, G. Kou, Y. Dong, F. Chiclana, E. Herrera-Viedma, A review on trust propagation and opinion dynamics in social networks and group decision making frameworks, Inform. Sci. 478 (2019) 461–475.

[3] J. Wu, F. Chiclana, H. Fujita, E. Herrera-Viedma, A visual interaction consensus model for social network group decision making with trust propagation, Knowl.-Based Syst. 122 (2017) 39–50.

[4] J. Wu, S. Wang, F. Chiclana, E. Herrera-Viedma, Two-fold personalized feedback mechanism for social network consensus by uninorm interval trust propagation, IEEE Trans. Cybern. 52 (10) (2021) 11081–11092.

[5] Q. Zha, X. He, M. Zhan, N. Lang, Managing consensus in balanced networks based on opinion and trust/distrust evolutions, Inform. Sci. (2023) 119223.

[6] S.M. Yu, Z.J. Du, X.Y. Zhang, H.Y. Luo, X.D. Lin, Trust Cop-Kmeans clustering analysis and minimum-cost consensus model considering voluntary trust loss in social network large-scale decision-making, IEEE Trans. Fuzzy Syst. 30 (7) (2021) 2634–2648.

[7] P. Liu, Y. Li, P. Wang, Opinion dynamics and minimum adjustment-driven consensus model for multi-criteria large-scale group decision making under a novel social trust propagation mechanism, IEEE Trans. Fuzzy Syst. (2022).

[8] Y. Dong, Q. Zha, H. Zhang, F. Herrera, Consensus reaching and strategic manipulation in group decision making with trust relationships, IEEE Trans. Syst. Man Cybern. 51 (10) (2020) 6304–6318.

[9] T.D. Huynh, Trust and Reputation in Open Multi-Agent Systems (Doctoral dissertation), University of Southampton, 2006.

[10] S.R. Yan, X.L. Zheng, Y. Wang, W.W. Song, W.Y. Zhang, A graph-based comprehensive reputation model: Exploiting the social context of opinions to enhance trust in social commerce, Inform. Sci. 318 (2015) 51–72.

[11] L. Chang, Y. Ouzrout, A. Nongaillard, A. Bouras, Z. Jiliu, Multi-criteria decision making based on trust and reputation in supply chain, Int. J. Prod. Econ. 147 (2014) 362–372.

[12] R. Urena, F. Chiclana, E. Herrera-Viedma, DeciTrustNET: A graph based trust and reputation framework for social networks, Inf. Fusion 61 (2020) 101–112.

[13] R. Monastersky, The Number that's Devouring Science, The Chronicle of Higher Education, 2005.

[14] L. Page, S. Brin, R. Motwani, T. Winograd, The PageRank Citation Ranking: Bringing Order to the Web, Technical Report, Stanford University, 1998.

[15] B. Liu, Q. Zhou, R.X. Ding, I. Palomares, F. Herrera, Large-scale group decision making model based on social network analysis: Trust relationship-based conflict detection and elimination, European J. Oper. Res. 275 (2) (2019) 737–754.

[16] H. Zhang, I. Palomares, Y. Dong, W. Wang, Managing non-cooperative behaviours in consensus-based multiple attribute group decision making: An approach based on social network analysis, Knowl.-Based Syst. 162 (2018) 29–45.

[17] Z. Gong, H. Wang, W. Guo, Z. Gong, G. Wei, Measuring trust in social networks based on linear uncertainty theory, Inform. Sci. 508 (2020) 154–172.

[18] J. Caverlee, L. Liu, S. Webb, The SocialTrust framework for trusted social information management: Architecture and algorithms, Inform. Sci. 180 (1) (2010) 95–112.

[19] A. Tajeddine, A. Kayssi, A. Chehab, H. Artail, Fuzzy reputation-based trust model, Appl. Soft Comput. 11 (1) (2011) 345–355.

[20] Y. Dong, Y. Li, Y. He, X. Chen, Preference–approval structures in group decision making: Axiomatic distance and aggregation, Decis. Anal. 18 (4) (2021) 273–295.

[21] Z. Zhang, Z. Li, Consensus-based TOPSIS-Sort-B for multi-criteria sorting in the context of group decision-making, Ann. Oper. Res. 325 (2) (2023) 911–938.

[22] Q. Zha, Y. Dong, F. Chiclana, E. Herrera-Viedma, Consensus reaching in multiple attribute group decision making: a multi-stage optimization feedback mechanism with individual bounded confidences, IEEE Trans. Fuzzy Syst. 30 (8) (2021) 3333–3346.

[23] C.C. Li, Y. Dong, Y. Xu, F. Chiclana, E. Herrera-Viedma, F. Herrera, An overview on managing additive consistency of reciprocal preference relations for consistency-driven decision making and fusion: Taxonomy and future directions, Inf. Fusion 52 (2019) 143–156.

[24] H. Zhang, C.C. Li, Y. Liu, Y. Dong, Modeling personalized individual semantics and consensus in comparative linguistic expression preference relations with self-confidence: An optimization-based approach, IEEE Trans. Fuzzy Syst. 29 (3) (2019) 627–640.

[25] H. Zhang, S. Zhao, G. Kou, C.C. Li, Y. Dong, F. Herrera, An overview on feedback mechanisms with minimum adjustment or cost in consensus reaching in group decision making: Research paradigms and challenges, Inf. Fusion 60 (2020) 65–79.

[26] F. Ji, J. Wu, F. Chiclana, S. Wang, H. Fujita, E. Herrera-Viedma, The overlapping community driven feedback mechanism to support consensus in social network group decision making, IEEE Trans. Fuzzy Syst. (2023) http://dx.doi.org/10.1109/TFUZZ.2023.3241062.

[27] Y. Dong, Q. Zha, H. Zhang, G. Kou, H. Fujita, F. Chiclana, E. Herrera-Viedma, Consensus reaching in social network group decision making: Research paradigms and challenges, Knowl.-Based Syst. 162 (2018) 3–13.

[28] A. Jøand, R. Ismail, The beta reputation system, in: Proceedings of the 15th Bled Electronic Commerce Conference, Vol. 5, 2002, pp. 2502–2511.

[29] N. Griffiths, Task delegation using experience-based multi-dimensional trust, in: Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems, 2005, pp. 489–496.

[30] L. Mui, M. Mohtashemi, A. Halberstadt, A computational model of trust and reputation, in: Proceedings of the 35th Annual Hawaii International Conference on System Sciences, IEEE, 2002, pp. 2431–2439.

[31] A.E. Arenas, B. Aziz, G.C. Silaghi, Reputation management in collaborative computing systems, Secur. Commun. Netw. 3 (6) (2010) 546–564.

[32] Dellarocas C., The digitization of word of mouth: Promise and challenges of online feedback mechanisms, Manag. Sci. 49 (10) (2003) 1407–1424.

[33] A. Whitby, A. Jøsang, J. Indulska, Filtering out unfair ratings in bayesian reputation systems, in: Proc. 7th Int. Workshop on Trust in Agent Societies, Vol. 6, 2004, pp. 106–117.

[34] W.L. Teacy, J. Patel, N.R. Jennings, M. Luck, Travos: Trust and reputation in the context of inaccurate information sources, Auton. Agents Multi-Agent Syst. 12 (2006) 183–198.

[35] M. Sensoy, J. Zhang, P. Yolum, R. Cohen, Poyraz: Context-aware service selection under deception, Comput. Intell. 25 (4) (2009) 335–366.

[36] D.G. Mikulski, F.L. Lewis, E.Y. Gu, G.R. Hudas, Trust dynamics in multi-agent coalition formation, in: Unmanned Systems Technology XIII, Vol. 8045, SPIE, 2011, pp. 252–266.

[37] 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, 2003, pp. 640–651.
[38] F. Herrera, E. Herrera-Viedma, L. Martínez, A fuzzy linguistic methodology to deal with unbalanced linguistic term sets, IEEE Trans. Fuzzy Syst. 16 (2) (2008) 354–370.
[39] R. Jurca, B. Faltings, Towards incentive-compatible reputation management, in: Workshop on Deception, Fraud and Trust in Agent Societies, Springer, Berlin, Heidelberg, 2002, pp. 138–147.
[40] M. Feldman, C. Papadimitriou, J. Chuang, I. Stoica, Free-riding and whitewashing in peer-to-peer systems, in: Proceedings of the ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems, 2004, pp. 228–236.
[41] M. Srivatsa, L. Xiong, L. Liu, TrustGuard: countering vulnerabilities in reputation management for decentralized overlay networks, in: Proceedings of the 14th International Conference on World Wide Web, 2005, pp. 422–431.
[42] Y.L. Sun, Z. Han, W. Yu, K.R. Liu, Attacks on trust evaluation in distributed networks, in: 2006 40th Annual Conference on Information Sciences and Systems, IEEE, 2006, pp. 1461–1466.
[43] Dellarocas C., Immunizing online reputation reporting systems against unfair ratings and discriminatory behaviour, in: Proceedings of the 2nd ACM Conference on Electronic Commerce, 2000, pp. 150–157.
[44] J. Weng, C. Miao, A. Goh, An entropy-based approach to protecting rating systems from unfair testimonies, IEICE Trans. Inf. Syst. 89 (9) (2006) 2502–2511.
[45] W. You, L. Liu, M. Xia, C. Lv, Reputation inflation detection in a Chinese C2C market, Electron. Commer. Res. Appl. 10 (5) (2011) 510–519.
[46] Y. Yang, Y.L. Sun, S. Kay, Q. Yang, Defending online reputation systems against collaborative unfair raters through signal modeling and trust, in: Proceedings of the 2009 ACM Symposium on Applied Computing, 2009, pp. 1308–1315.
[47] D.H. McKnight, V. Choudhury, C. Kacmar, Developing and validating trust measures for e-commerce: An integrative typology, Inf. Syst. Res. 13 (3) (2002) 334–359.
[48] C.N. Ziegler, J. Golbeck, Investigating interactions of trust and interest similarity, Decis. Support Syst. 43 (2) (2007) 460–475.
[49] L. Xiong, L. Liu, Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities, IEEE Trans. Knowl. Data Eng. 16 (7) (2004) 843–857.
[50] R.R. Yager, Quantifier guided aggregation using OWA operators, Int. J. Intell. Syst. 11 (1) (1996) 49–73.
[51] Notice of shandong provincial department of finance on issuing rules for the selection of government procurement experts in shandong province, Bull. Shandong Provincial People's Govern. (33) (2017) 59–62, (in Chinese).
[52] Notice of Beijing municipal science and technology commission on printing and distributing the management measures of Beijing science and technology expert database (trial implementation), Bull. Beijing Municipal People's Govern. (17) (2020) 5–14, (in Chinese).
[53] M. Fishbein, I. Ajzen, A. Belief, Intention and behaviour: An introduction to theory and research, 1975.
[54] E. Chang, F. Hussain, T. Dillon, Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence, John Wiley & Sons, 2006.
[55] Y. Wang, D.S. Wong, K.J. Lin, V. Varadharajan, Evaluating transaction trust and risk levels in peer-to-peer e-commerce environments, Inf. Syst. E-Bus. Manag. 6 (1) (2008) 25–48.
[56] V. Deora, J. Shao, W. Gray, J. Fiddian, A quality of service management framework based on user expectations, in: The International Conference on Service-Oriented Computing, ICSOC, Trento, Italie, 2003, pp. 104–114.
[57] J. Sabater, C. Sierra, Social regret, a reputation model based on social relations, ACM SIGecom Exch. 3 (1) (2001) 44–56.
[58] B. Khosravifar, J. Bentahar, M. Gomrokchi, R. Alam, CRM: An efficient trust and reputation model for agent computing, Knowl.-Based Syst. 30 (2012) 1–16.
[59] P. Massa, P. Avesani, Controversial experts demand local trust metrics: An experimental study on epinions. com community, in: AAAI Vol. 1, 2005, pp. 121–126.
[60] K.K. Fullam, T.B. Klos, G. Muller, J. Sabater, A. Schlosser, Z. Topol, et al., A specification of the agent reputation and trust (art) testbed: experimentation and competition for trust in agent societies, in: Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems, pp. 512–518.