A Trust Risk Dynamic Management Mechanism Based on Third-Party Monitoring for the Conflict-Eliminating Process of Social Network Group Decision Making

Mengqi Li, Yejun Xu, Xia Liu, Francisco Chiclana, and Francisco Herrera, *Senior Member, IEEE*

***Abstract*—Every decision may involve risks. Real-world risk issues are usually supervised by third parties. Decision-making may be affected by the absence of sufficient or reasonable trust or to the opposite, an unconditional, excessive, or blind trust, which is called trust risks. The conflict-eliminating process (CEP) aims to facilitate satisfactory consensus by decision makers (DMs) through continuous reconciliation between their opinion differences on the subject matter. This article addresses trust risks in CEP of social network group decision making (SNGDM) through third-party monitoring. A trust risk analysis-based conflict-eliminating model for SNGDM is developed. It is assumed that a third-party agency monitors the DMs' credibility and performance, which is recorded in an objective evaluation matrix and multi-attribute trust assessment matrix (MTAM). A trust risk measurement methodology is proposed to classify the DMs' different trust risk types and to measure the trust risk index (TRI) of a group of DMs. When TRI is unacceptable, a trust risk management mechanism that controls TRI is activated. Different management policies are applicable to DMs' different trust risk types. There are two main methods: 1) dynamically update the MTAM based on DMs' performance and 2) provide suggestions for modifying the DM's information with high TRI. Besides, as part of the integrated CEP, this model includes an optimization approach to dynamically derive DMs' reliable aggregation weights from their MTAM. Simulation experiments and an illustrative example support the feasibility and validity of the proposed model for managing trust risks in CEP of SNGDM.**

***Index Terms*—Conflict-eliminating process (CEP), group decision making (GDM), social network (SN), third party, trust risk.**

Manuscript received November 23, 2020; revised July 30, 2021 and January 27, 2022; accepted March 9, 2022. This work was supported in part by the Postgraduate Research & Practice Innovation Program of Jiangsu Province under Grant KYCX20_0507; in part by the Fundamental Research Funds for the Central Universities under Grant B200203165 and Grant B220203013; in part by the National Natural Science Foundation of China (NSFC) under Grant 71871085; in part by the National Natural Science Foundation of Jiangsu Province under Grant BK20210634; in part by the Startup Foundation for Introducing Talent of NUIST under Grant 1521182101004; and in part by the China Scholarship Council under Grant 202106710123. This article was recommended by Associate Editor Z. Xu. *(Corresponding author: Yejun Xu.)*

Mengqi Li is with the Business School, Hohai University, Nanjing 211100, China, and also with the Andalusian Research Institute on Data Science and Computational Intelligence, University of Granada, 18071 Granada, Spain (e-mail: sdbzlm7@163.com).

Yejun Xu is with the College of Management and Economics, Tianjin University, Tianjin 300072, China (e-mail: xuyejohn@163.com).

Xia Liu is with the School of Management Science and Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: liu_xia523hn@163.com).

Francisco Chiclana is with the Andalusian Research Institute in Data Science and Computational Intelligence, University of Granada, 18071 Granada, Spain, and also with the Institute of Artificial Intelligence, School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, U.K. (e-mail: chiclana@dmu.ac.uk).

Francisco Herrera is with the Andalusian Research Institute on Data Science and Computational Intelligence, University of Granada, 18071 Granada, Spain, and also with the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: herrera@decsai.ugr.es).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCYB.2022.3159866.

Digital Object Identifier 10.1109/TCYB.2022.3159866

I. Introduction

With the progress of intelligent decision making, modeling of social network (SN) group decision making (SNGDM) has been an attractive topic [1]. The SNGDM process can be briefly described as follows: decision makers (DMs) voice their opinions with respect to multiple alternatives for a common decision problem on an SN platform and seek out their collective optimal solution. At the initial stage of the SNGDM process, DMs may have conflicting views. Consequently, a conflict-eliminating process (CEP) is required to reach satisfactory consensus among DMs [1], [2]. The traditional CEP framework includes five pivotal elements: 1) preference representation; 2) aggregation; 3) measurement of conflict level; 4) feedback mechanism; and 5) selection process. Different from traditional scenarios, SNs have the advantages of collaboration, information sharing, convenient communication and interoperability [3]. There are two types of consensus models for eliminating conflicts among DMs in SNGDM that have been extensively studied: 1) conflict-eliminating model based on trust relationships [4] and 2) conflict-eliminating model based on opinion evolution [1], [5].

In SNGDM, trust relationships among DMs are regarded as the critical components of CEP. On the one hand, trust is a key factor reflecting the status and importance of DMs in the SN, and can be explicitly used to derive the aggregation weights of DMs [5]. On the other hand, trust-based feedback is considered to be a more acceptable feedback strategy for DMs [4]. Classically, the measurement of trust relationships among DMs in the SN has two characteristics:

1) matrix representation is used to model trust relationships among DMs in an SN, which is deemed as a reliable source to calculate the trust degrees (TDs) of DMs [6] and 2) trust is generally considered static and immutable in SNGDM [7], which also makes the aggregation weights of DMs in CEP static or fixed throughout the SNGDM processes. Whereas, this weights derivation method based on TDs dose not conform to the dynamic changes of actual decision-making situation and needs to be remedied.

Although many trust-based conflict-eliminating models have been developed in SNGDM, they have usually overlooked an established fact: trust is always accompanied by risks [8], [9]. At present, most researches on trust risks focus on the fields of economy, finance and e-commerce. In SNGDM, only the trust transitivity research that integrates the DMs' risk attitude [10] has been covered, with no implementation of the trust risk issues into CEP. In real-world SNGDM, DMs' credibility may be different from the TDs obtained from SN, which means that DMs' credibility does not match their status and importance in the SN. In this case, some DMs may be blindly trusted or lack due trust, which is called trust risks. Ultimately, they may mislead the public and affect the reliability and credibility of decision result. However, to our knowledge, the existing trust-based CEPs in SNGDM often ignore the assessment of DMs' different credibility, and do not conduct quantitative analysis and management of trust risks.

The above analysis shows that there are still some key aspects of CEP in SNGDM that need further investigation.

1) *Credibility Assessment:* As the main input information, the credibility of DMs' information plays a key role in decision making. DMs' different knowledge backgrounds or interest imply that their preferences and credibility are also different. Coupled with the anonymity and openness of SNs, the credibility assessment of DMs and their information may lack strong supervision in the decision-making process [11]. Hence, finding a reliable methodology to evaluate the credibility of DMs in CEP is a challenging problem.
2) *Dynamic Derivation of DMs' Weights:* The openness of SNs and the interaction of decision information requires the distribution of DMs' weights to be dynamic rather than fixed and static. Meanwhile, the role of DMs' credibility in the weight generation process cannot be ignored. This is because a DM with high credibility and high prestige in the SN should have a higher weight when gathering information. Consequently, within the considered dynamic interaction decision-making process, it is necessary to carry out research on the dynamic weight generation process based on the credibility and TDs of DMs.
3) *Trust Risk Measurement and Dynamic Management Mechanism in CEP:* DMs' cognition level or external temptations may result in DMs providing low credibility, biased, or misleading information. Naturally, DMs' TDs may not match their credibility, which gives rise to two trust risk issues: a) if the DM with low credibility has high TD because of her/his position in the SN, she/he may be blindly trusted or overtrusted by others and b) if a DM who provides reasonable and reliable information has a lower status in the SN, she/he may lack sufficient trust. Obviously, DMs with blind trust or lack of appropriate trust may mislead other members of the group, resulting in misleading and unfair decision results. Thus, to ensure the credibility and reliability of the final decision, it is urgent to measure and dynamically manage the trust risk issues in CEP of SNGDM.

Motivated by these problems, this study establishes a novel conflict-eliminating framework with trust risk dynamic management mechanism to manage trust risks and promote consensus. The proposed methodology contains the following key features.

1) A third-party agency is introduced to monitor and evaluate the performance and trustworthiness of DMs. In fact, the credibility evaluation of DMs cannot be given by themselves since self-evaluation is easy to be unfair. Hence, the credibility evaluation by a fair and neutral third-party organization becomes a valid approach [12]. Thus, DMs will share their information with the third party so that they can correctly hold and understand DMs' information at each CEP round to help the assessment of the performance and trustworthiness of DMs. Furthermore, the third party can realize trust risk management and optimize CEP by influencing the DMs' preferences. Based on the above analysis and inspired by the work by Wu *et al.* [13], the third-party regulatory agency should comply with the following hypotheses,

   Hypothesis 1: The third party is fair, impartial, reliable, and not driven by various interests in CEP.

   Hypothesis 2: The third party has in-depth knowledge of the DMs' information and performance at each CEP round.

   Herein, various factors that affect DMs' credibility, such as competence, consistency, fairness, integrity, and receptivity, are considered [14]. The evaluation information is offered by means of an objective evaluation matrix (OEM).
2) A dynamic weights generation process is designed. As per the third-party evaluation information, combined with TDs derived by SNs, a multi-attribute trust assessment matrix (MTAM) is constructed. Based on an optimization approach, DMs' weights are obtained from their MTAM and integrated into the CEP.
3) This is the first attempt to study the CEP with trust risk problems in SNGDM framework. To manage the trust risk issues in CEP, a novel trust risk measurement and dynamic management mechanism is developed. By measuring the deviation between the weight rankings of MTAM and OEM, the DMs' trust risk degrees and trust risk types are determined. Moreover, a trust risk index (TRI) is introduced to judge whether the trust risk degree of the group of DMs is acceptable or not. When TRI is unacceptable, the trust risk dynamic management mechanism is activated. The third party provides different strategies for DMs' different trust risk types: a) for a DM lacking sufficient trust, the MTAM is dynamically updated to provide compensation and rewards and b) for

a blindly trusted DM, while the MTAM is dynamically updated and punished, she/he is encouraged to modify her/his judgments based on the highly credible DM's information. This mechanism reduces the group TRI and guarantees the reliability of the decision results.

4) A new conflict elimination framework with trust risk dynamic management under the supervision of the third party is proposed. In this model, the third party measures and manages trust risk issues by monitoring DMs' performance and credibility. Through the dynamic update of the MTAM, the DMs' weights are dynamically allocated and applies in the CEP. Eventually, the proposed methodology reduces the group TRI while eliminating the conflict of DMs' opinions to allow the reaching of consensus. Some simulation experiments are designed to support the feasibility and validity of the proposal for handling trust risk issues in CEP of SNGDM. It is noted that trust risk issues are widespread phenomena in decision making, which becomes more obvious as the number of DMs increases. When TRI is high, the trust risk dynamic management mechanism is activated. A strict TRI threshold and an appropriate reward and punishment coefficient allow for the trust risk management to be more efficient and faster. Compared with the traditional CEP, it is found that the proposed dynamic management of trust risk issues in CEP can accelerate consensus and increase the success ratio of conflict elimination. From an application point of view, an illustrative example demonstrates how the proposed conflict resolution framework dynamically manages trust risks and eliminates conflicts of DMs' opinions in SNGDM. The results of this example support the claim that the proposed methodology provides decision support to address trust risk issues in real-world SNGDM, which ensures the rationality and reliability of the decision-making outcome.

The remainder of this article is organized as follows. Section II reviews some preliminaries and describes the trust risk problems in the CEP of SNGDM. In Section III, a new decision framework to address trust risk issues is developed. Trust risk measurement and dynamic management mechanism are also elaborated in this section. Section IV reports on the feasibility and validity of the proposed methodology with simulation experiments while Section V provides an illustrative example. Section VI summarizes the main research contributions as well as potential follow-up studies for future work.

II. Preliminaries

This section introduces basic knowledge on additive preference relations (APRs) and related properties, the selection process in group decision making (GDM), and trust relationships among DMs in SNs. In addition, the decision problem of interest, the CEP with trust risks in SNGDM, is described in Section II-D.

A. APRs

Herein, $X = \{x_1, x_2, \ldots, x_n\}$ $(n \geq 2)$ represents a finite set of alternatives, while $E = \{e_1, e_2, \ldots, e_m\}$ $(m \geq 2)$ represents a set of DMs who express their views using APRs as described below.

TABLE I
$\overline{\mathrm{GCI}}$ Threshold for APRs

CR	0.01	0.05	0.1	0.15
$\overline{GCI}(n=3)$	0.0314	0.1573	0.3147	0.4720
$\overline{GCI}(n=4)$	0.0352	0.1763	0.3526	0.5289
$\overline{GCI}(n>4)$	~0.037	~0.185	~0.370	~0.555

Definition 1 [15]: An APR on X is represented by a matrix $P = (p_{ij})_{n\times n}$, with elements p_{ij} being the preference degree in [0, 1] of alternative x_i over alternative x_j. An APR is often assumed to be reciprocity: $p_{ij} + p_{ji} = 1$, for all $i, j = 1, \ldots, n$.

Definition 2 [16]: An APR $P = (p_{ij})_{n\times n}$ is multiplicative consistent if it satisfies the property

$$p_{ij}p_{jk}p_{ki} = p_{ji}p_{kj}p_{ik}, \quad \text{for all } i, j, k = 1, \ldots, n. \tag{1}$$

Xia *et al.* [17] proposed the below geometric consistency index (GCI) to measure the multiplicative consistency of APRs

$$\mathrm{GCI}(P) = \frac{2}{(n-1)(n-2)} \sum_{i<j} \big(\ln p_{ij} - \ln p_{ji} - \ln w_i + \ln w_j\big)^2 \tag{2}$$

where $w = (w_1, w_2, \ldots, w_n)^T$, $w_i \in [0,\ 1]$ and $\sum_{i=1}^{n} w_i = 1$, is the priority weighting vector associated to P. According to the consistency ratio (CR) given by Saaty [18], Xu *et al.* [19] extended the GCI thresholds of multiplicative preference relations in [20] to obtain the corresponding thresholds of APRs (Table I). If $\mathrm{GCI}(P) \leq \overline{\mathrm{GCI}}$, P is of acceptable multiplicative consistency.

Definition 3 [21]: An APR $P = (p_{ij})_{n\times n}$ is ordinally consistent, if the following conditions are satisfied.

1) If $p_{ik} > 0.5$, $p_{kj} \geq 0.5$, or $p_{ik} \geq 0.5$, $p_{kj} > 0.5$, then $p_{ij} > 0.5$.
2) If $p_{ik} = 0.5$ and $p_{kj} = 0.5$, then $p_{ij} = 0.5$.

B. Selection Process

The selection process of GDM includes two stages.

1) *Aggregation Phase:* This phase aims to obtain a collective APR $P^{(c)} = (p_{ij}^{(c)})_{n\times n}$ by fusing all individual APRs $P^{(k)} = (p_{ij}^{(k)})_{n\times n}$, $k = 1, \ldots, m$. In this study, the weighted average (WA) operator is used to obtain the collective APR

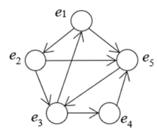
$$p_{ij}^{(c)} = WA\Big(p_{ij}^{(1)}, p_{ij}^{(2)}, \ldots, p_{ij}^{(m)}\Big) = \sum_{k=1}^{m} \lambda_k p_{ij}^{(k)} \tag{3}$$

where $\lambda_k \in [0,\ 1]$ is the weight of DM e_k subject to the normalization property $\sum_{k=1}^{m} \lambda_k = 1$.

2) *Exploitation Phase:* Once the collective APR is obtained, the exploitation stage is applied to derive the final ranking of alternatives. Inspired by the ordered weighted averaging (OWA) [22], the quantifier-guided dominance degree (QGDD) of alternatives based on the APR, P, measures the degree up to which one alternative dominates a "fuzzy majority" of the rest of alternatives, and it is defined as follows [23]:

$$QGDD(x_i) = \mathrm{OWA}_Q\big(p_{ij}, j = 1, \ldots, n\big). \tag{4}$$

TABLE II
DIFFERENT REPRESENTATION SCHEMES IN SNA

Sociometric	Graph	Algebraic
$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$		e_1Re_2, e_1Re_5, e_2Re_3, e_2Re_5, e_3Re_1, e_3Re_4, e_4Re_5, e_5Re_3.

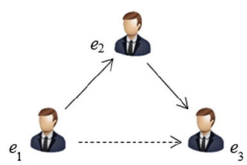


Fig. 1. Trust propagation via a trust path.

C. Trust Relationship Among DMs in Social Networks

Trust relationship among DMs is of great significance in any GDM process. It is generally regarded as a reliable information to obtain the aggregation weights of DMs [5]. SN analysis (SNA) is a common and effective tool to measure the trust relationship between DMs within a group [1]. The three components of SNA are: 1) the participants set; 2) the relationship between participants; and 3) the attributes of participants. Moreover, there are three frequently used approaches to show the set and relationships of participants (Table II).

1) *Sociometric:* Utilize two-ways matrices, called: a) sociomatrices or b) adjacency matrices, to express relationships among DMs in the SN.
2) *Graph:* Use a graph of nodes connected by directed edges to represent the relationships between relevant DMs in the SN.
3) *Algebraic:* Differentiate several unique relationships and signify different combinations of relationships.

To appropriately express trust relationships in SNA, a fuzzy sociometric is proposed to model the uncertainty of trust relationships, thereby improving the accuracy of description [24].

Definition 4 [24]: A fuzzy sociometric on E, S, is a relation on $E \times E$, $S : E \times E \to [0,\ 1]$, where $S(e_k, e_h) = s_{kh} \in [0,\ 1]$ measures the extent up to which e_k is related to e_h. In particular, $s_{kh} = 1$ or 0 means that e_k is absolutely related to e_h or e_k is independent of e_h, respectively.

In actual SNGDM problems, there might be a direct or indirect trust relationship between each pair of DMs. For instance, in Fig. 1, e_1 and e_3 have no direct trust relationship. However, the missing trust value between e_1 and e_3 can be evaluated/estimated using the indirect trust path $(e_1e_2)(e_2e_3)$. To estimate the indirect trust values in the SN, a trust propagation method based on the t-norm operator is presented.

Definition 5 [3]: Assuming that $e_k \overset{1}{\to} e_{(1)} \overset{2}{\to} \cdots \overset{q}{\to} e_{(q)} \overset{q+1}{\to} e_h$ is a trust path of length $q+1$ from e_k to e_h, the trust value s_{kh} is obtained by the t-norm operator as follows:

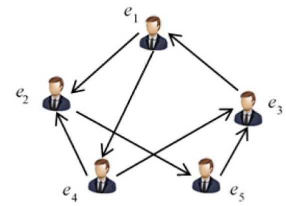


Fig. 2. SN structure among five DMs in an SNGDM problem.

$$\begin{aligned} s_{kh} &= TN\big(s_{k,\sigma(1)}, s_{\sigma(1),\sigma(2)}, \ldots, s_{\sigma(q),h}\big) \\ &= \frac{2s_{k,\sigma(1)} \cdot s_{\sigma(q),h} \prod_{z=1}^{q-1} s_{\sigma(z),\sigma(z+1)}}{\big(2-s_{k,\sigma(1)}\big)\big(2-s_{\sigma(q),h}\big) \prod_{z=1}^{q-1}\big(2-s_{\sigma(z),\sigma(z+1)}\big)+s_{k,\sigma(1)} \cdot s_{\sigma(q),h} \prod_{z=1}^{q-1} s_{\sigma(z),\sigma(z+1)}}. \end{aligned} \tag{5}$$

There may be multiple trust paths available between pairs of DMs in the SN [1], [7]. Thus, the overall TD for each pair of DMs is computed using the trust aggregation based on the OWA operator [7]. Assuming κ trust paths between e_k and e_h, with corresponding trust values $s_{kh}^1, \ldots, s_{kh}^\kappa$, the trust value between e_k and e_h, s_{kh}, is estimated using expression

$$s_{kh} = \mathrm{OWA}_Q\Big(s_{kh}^1, \ldots, s_{kh}^\kappa\Big) = \sum_{z=1}^{\kappa} \pi_z s_{kh}^{\sigma(z)} \tag{6}$$

where $s_{kh}^{\sigma(z)}$ is the zth largest value in $\{s_{kh}^1, \ldots, s_{kh}^\kappa\}$, and $\pi = (\pi_1, \pi_2, \ldots, \pi)^T$ is a weight vector verifying $\pi_z \in [0,\ 1]$ and $\sum_{z=1}^{\kappa} \pi_z = 1$.

When all trust values by indirect trust in the SN are estimated and supplemented, a complete fuzzy sociometric S is constructed. Furthermore, Liu *et al.* [7] proposed the following method to measure the TD of each DM in the SN.

Definition 6 [7]: Assume that $S = (s_{kh})_{m\times m}$ is a complete fuzzy sociometric matrix. The TD of e_h, $\mathrm{TD}(e_h)$, is

$$\mathrm{TD}(e_h) = \frac{1}{m-1} \sum_{k=1, k\neq h}^{m} s_{kh}, \quad h = 1, 2, \ldots, m. \tag{7}$$

Example 1: Suppose the set of five DMs $E = \{e_1, e_2, \ldots, e_5\}$ shown in Fig. 2. Assume the following fuzzy sociometric:

$$S = \begin{pmatrix} - & 0.6 & 0 & 0.7 & 0 \\ 0 & - & 0 & 0 & 0.7 \\ 0.6 & 0 & - & 0 & 0 \\ 0 & 0.8 & 0.9 & - & 0 \\ 0 & 0 & 0.8 & 0 & - \end{pmatrix}.$$

Considering the propagation and aggregation of trust in the SN, the complete fuzzy sociometric by (5) and (6) is

$$S = \begin{pmatrix} - & 0.6 & 0.28 & 0.7 & 0.26 \\ 0.27 & - & 0.53 & 0.15 & 0.7 \\ 0.6 & 0.28 & - & 0.38 & 0.16 \\ 0.32 & 0.8 & 0.9 & - & 0.3 \\ 0.44 & 0.16 & 0.8 & 0.27 & - \end{pmatrix}.$$

Using (7), the TDs of the five DMs are: $\mathrm{TD}(e_1) = 0.41$, $\mathrm{TD}(e_2) = 0.46$, $\mathrm{TD}(e_3) = 0.63$, $\mathrm{TD}(e_4) = 0.38$, and $\mathrm{TD}(e_5) = 0.36$.

D. Decision Problem (CEP With Trust Risks in SNGDM)

As mentioned in Section I, there are two trust risk situations for DMs in CEP: 1) DM is at risk of being blindly trusted, and 2) a DM lacks the trust she/he deserves. Below, we introduce the SNGDM problems under trust risk situations.

We assume a set of SN-related DMs E who provide APRs $P^{(k)} = (p_{ij}^{(k)})_{n\times n}$, $k = 1, \ldots, m$, on X. Due to their different knowledge backgrounds or interest, the ranking of DMs' credibility and the ranking of DMs' weighs may be inconsistent. Hence, some DMs may be blindly trusted or may lack reasonable trust in CEP. The question to investigate is how to help DMs address these trust risk issues, eliminate the conflict of their opinions and reach a consensus in SNGDM.

III. New Conflict Elimination Framework to Cope With Trust Risk Issues in SNGDM

This section develops a model to manage the mentioned trust risk issues in the CEP of SNGDM. Section III-A presents a solution framework. Section III-B discusses the factors that may cause trust risk issues and develop a trust risk measurement approach. Afterward, a trust risk dynamic management mechanism is proposed in Section III-C.

A. Novel Solution Framework

To address the trust risk issues in CEP, a new conflict resolution framework is developed. This model includes a third-party organization to monitor and objectively evaluate the performance and credibility of DMs. It aims to measure and process the trust risk problems and to ensure the authenticity and rationality of the decision results. Meanwhile, the DMs' weights are dynamically generated as per their performance evaluation in CEP. Thus, the conflict-eliminating framework for managing trust risks has five phases: 1) dynamic weights generation process; 2) trust risk measurement and dynamic management mechanism; 3) conflict level measurement; 4) feedback mechanism; and 5) selection process. These are depicted in Fig. 3 and described next.

1) Dynamic Generation of DMs' Weights: This phase is based on an optimization-based methodology to dynamically derive DMs' weights from the third-party evaluation information.

During CEP, the OEM and MTAM are used for recording third-party evaluation information. In each CEP round, the third party dynamically updates the OEM and MTAM by monitoring DMs' credibility and performance when facing decision problems. Meanwhile, an optimization model is constructed to compute DMs' weights from their evaluation information. In what follows, we take the MTAM as an example to illustrate the process of building the evaluation information and dynamically deriving DMs' weights.

Let $C = \{c_1, c_2, \ldots, c_l\}$ $(l \geq 2)$ be a set of attributes involving trust (the composition of these possible attributes is discussed in Section III-B) with weighting vector $\eta = (\eta_1, \ldots, \eta_l)^T$ such that $\eta_j \geq 0$ and $\sum_{j=1}^{l} \eta_j = 1$. Let the third party's MTAM evaluation of DMs, e_k, with respect to attributes, c_j, be $T = (t_{kj})_{m\times l}$.

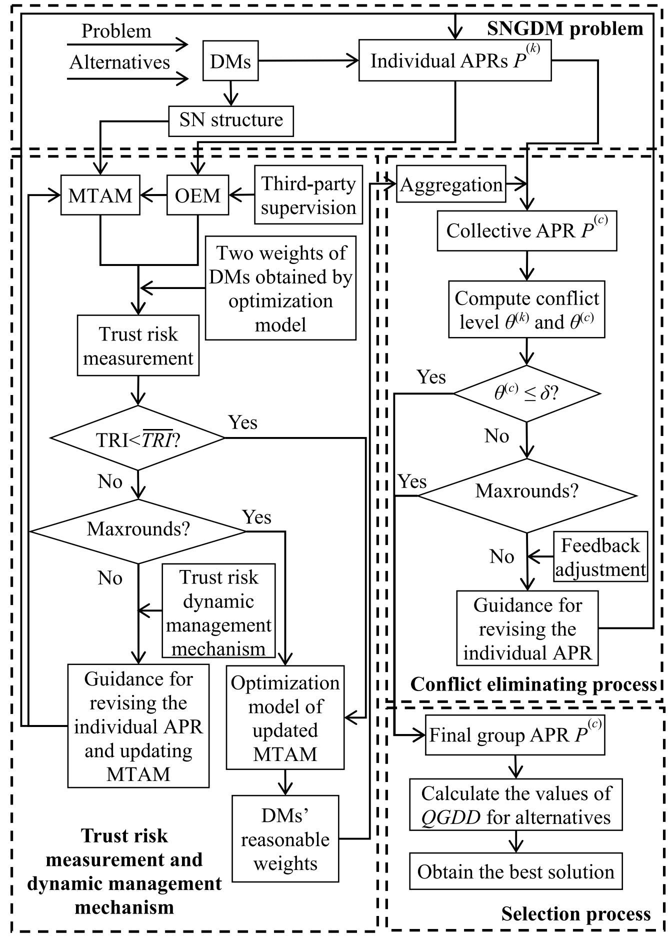


Fig. 3. Framework of SNGDM with trust risk problems.

First, using cost-benefit attributes normalization process, the third party's MTAM is normalized $\bar{T} = (\bar{t}_{kj})_{m\times l}$:

$$\bar{t}_{kj} = \frac{1/t_{kj}}{\sum_{k=1}^{m}(1/t_{kj})}, \text{ for cost attribute } c_j,\ j = 1, 2, \ldots, l \quad (8)$$

$$\bar{t}_{kj} = \frac{t_{kj}}{\sum_{k=1}^{m} t_{kj}}, \text{ for benefit attribute } c_j,\ j = 1, 2, \ldots, l. \quad (9)$$

Let $\lambda = (\lambda_1, \ldots, \lambda_m)^T$ be the weighting vector of DMs, where $\lambda_k \geq 0$ is the weight of DM e_k and $\sum_{k=1}^{m} \lambda_k = 1$. To obtain a reasonable weight distribution of DMs, the third party's synthetical assessed value of DM e_k is obtained by fully combining all potential attributes that affect trust: $\mu_k = \sum_{j=1}^{l} \eta_j \bar{t}_{kj}$. The value of μ_k denotes the trustworthiness of DM e_k; the larger the value of μ_k, the more credible and important DM e_k is. The deviation between μ_k and λ_k is measured as the square of their difference $(\mu_k - \lambda_k)^2$, and the total deviation of all DMs will be $\sum_{k=1}^{m}(\mu_k - \lambda_k)^2$. To keep the total deviation as small as possible, the following nonlinear programming model is established:

$$\textbf{(M-1)}\ \min \sum_{k=1}^{m}\left(\sum_{j=1}^{l} \eta_j \bar{t}_{kj} - \lambda_k\right)^2$$
$$\text{s.t.} \begin{cases} \sum_{k=1}^{m} \lambda_k = 1 \\ \lambda_k \geq 0, k = 1, \ldots, m. \end{cases}$$

Theorem 1: The unique optimal solution of $(M-1)$ is

$$\lambda_k = \sum_{j=1}^{l} \eta_j \bar{t}_{kj}, \quad k = 1, \ldots, m. \tag{10}$$

Proof: Consider the Lagrange function

$$L(\lambda_k, \rho) = \sum_{k=1}^{m} \left(\sum_{j=1}^{l} \eta_j \bar{t}_{kj} - \lambda_k \right)^2 + \rho \left(\sum_{k=1}^{m} \lambda_k - 1 \right)$$

where ρ is the Lagrange multiplier. Setting the partial derivatives of L equal to zero, we have

$$\frac{\partial L(\lambda_k, \rho)}{\partial \lambda_k} = -2 \left(\sum_{j=1}^{l} \eta_j \bar{t}_{kj} - \lambda_k \right) + \rho = 0 \tag{11}$$

and

$$\frac{\partial L(\lambda_k, \rho)}{\partial \rho} = \sum_{k=1}^{m} \lambda_k - 1 = 0. \tag{12}$$

Solving (11), we obtain

$$\lambda_k = \sum_{j=1}^{l} \eta_j \bar{t}_{kj} - \frac{\rho}{2}. \tag{13}$$

Then, substituting (13) into (12), we obtain $\sum_{k=1}^{m} \sum_{j=1}^{l} \eta_j \bar{t}_{kj} - \frac{\rho m}{2} = 1$. As per (8) and (9), we have $\sum_{k=1}^{m} \sum_{j=1}^{l} \eta_j \bar{t}_{kj} = \sum_{j=1}^{l} \eta_j \sum_{k=1}^{m} \bar{t}_{kj} = \sum_{j=1}^{l} \eta_j = 1$. Hence, $\rho = 0$. Subsequently, based on (13), we have $\lambda_k = \sum_{j=1}^{l} \eta_j \bar{t}_{kj}$, $k = 1, \ldots, m$. This completes the proof of Theorem 1.

2) Trust Risk Measurement and Dynamic Management Mechanism: This phase considers the potential factors affecting DMs' credibility in a comprehensive way. Under the supervision of the third party, the types and degrees of trust risk for DMs can be accurately judged, and the group TRI can be tested. By means of dynamic management measures, TRI is finally controlled within an acceptable range. Sections III-B and III-C present the details of trust risk measurement and dynamic management, respectively.

3) Measurement of Conflict Degree: Conflict degree is employed to measure the difference between the DMs' APRs and the collective APR. The conflict degree is defined as follow.

Definition 7: Let $P^{(k)} = (p_{ij}^{(k)})_{n\times n}$, $k = 1, \ldots, m$, be the k^{th} individual APR, and $P^{(c)} = (p_{ij}^{(c)})_{n\times n}$ is the collective APR obtained by (3). The conflict degree between $P^{(k)}$ and $P^{(c)}$ is measured in [0, 1] as follows:

$$\theta^{(k)} = \frac{2}{n(n-1)} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \left| p_{ij}^{(k)} - p_{ij}^{(c)} \right|. \tag{14}$$

The greater the value of $\theta^{(k)}$, the higher the conflict level between $P^{(k)}$ and $P^{(c)}$. When $\theta^{(k)} = 0$, there is no conflict between $P^{(k)}$ and $P^{(c)}$. The maximum conflict between $P^{(k)}$ and $P^{(c)}$ happens when only 0-1 preference values are permitted and one APR is the complement of the other APR in the classical sense, that is, $P^{(k)} = 1 - P^{(c)}$.

The group conflict degrees $\theta^{(c)}$ is computed in [0, 1] as

$$\theta^{(c)} = \sum_{k=1}^{m} \lambda_k \theta^{(k)}. \tag{15}$$

A large value of $\theta^{(c)}$ indicates a high conflict degree among DMs. Unless a DM is allocated a null weight value, when $\theta^{(c)} = 0$, the DMs' individual APR $P^{(k)}$ will coincide and be the same as the group's preference. This is an unlikely scenario in practice for a group of heterogeneous DMs, and in the case of this scenario to be possible the decision problem would be an individual decision-making problem rather than a GDM problem, with trust/distrust/SN not playing any role. Generally, an acceptable threshold of group conflict level δ will be tolerated in practice. This can be formulated as: if $\theta^{(c)} \leq \delta$, the group reaches an acceptable level of conflict, and the selection process of the decision-making process can initiate. Otherwise, a feedback mechanism is activated to reduce the group conflict degree to the acceptable threshold of group conflict level.

4) Feedback Mechanism: The aim of the feedback adjustment mechanism is to provide support to DMs on adjusting their preference information to reduce the group conflict level. To achieve a consensus, DMs are encouraged to modify their opinions automatically, which includes the following two steps.

1) *Identification of the DM With Highest Conflict Level:* The DM with highest conflict degree has the largest deviation from group's views. In other words, the opinions provided by this DM has a negative impact on CEP. Therefore, the DM e_k with maximum value of $\theta^{(k)}$ at each round of feedback is provided support for modifying her/his preferences. In the case of being more than one DM with highest conflict level value, then any of them is (randomly) selected.
2) *Adjustment Process:* The APR $\bar{P}^{(k)} = (\bar{p}_{ij}^{(k)})_{n\times n}$ obtained from modifying the APR $P^{(k)}$ of the identified DM with highest conflict level, e_k, is obtained based on the following recommendation rules:

$$\begin{cases} \bar{p}_{ij}^{(k)} = (1-\xi)p_{ij}^{(k)} + \xi p_{ij}^{(c)}, & i \leq j, k = 1, \ldots, m, 0 \leq \xi \leq 1 \\ \bar{p}_{ji}^{(k)} = 1 - \bar{p}_{ij}^{(k)}, & i > j \end{cases} \tag{16}$$

where ξ is a modification and fusion coefficient in [0, 1].

Remark 1: The above feedback process is an automated approach, and is applied until the group conflict degree is within the acceptable threshold of group conflict level. It would promote consensus effectively only if the recommended rules are implemented in each round of CEP. However, an extreme situation is that the DM with highest conflict degree is unwilling to change her/his preferences as per the recommendation rules, which is a negative decision behavior and is not conducive to CEP. In this case, the DM can be allowed to adjust her/his APR more freely to increase her/his enthusiasm and initiative. It should be noted that her/his new APR is considered valid only when the conflict degree of the new APR is lower than its current conflict degree. Otherwise, it is strongly recommended that this DM follows the given rules to provide a new APR. For an identified DM who does not modify preferences and does not cooperate to promote consensus, her/his APR are discarded in SNGDM.

5) Selection Process: After DMs have eliminated conflicts and reach an agreement, the selection process (Section II-B) is applied to derive the final ranking of decision alternatives from the group's opinion.

B. Measurement of Trust Risk

Butler [14] indicated the following factors related to trust: competence, consistency, integrity, fairness, and receptivity. Here, we introduce them into CEP and utilize them as the third-party criteria for measuring the DMs' credibility based on their performance, and for providing objective evaluation information. In the following, we analyze these factors and explain the situations that may lead to trust risk problems.

1) Factor I (Competence): From the DMs' perspective, their competence can be captured with the ordinal consistency of their preferences. Ordinal consistency is the minimum requirement to ensure logic and rational DMs' preferences, which reflects the DMs' understanding and intelligence with regard to the given decision problem. An incompetent DM should be given less credit than a competent one because of her/his illogical understanding for the SNGDM problem. If she/he is assigned too much trust, it may lead to wrong decisions.

Let $P^{(k,t)} = (p_{ij}^{(k,t)})_{n\times n}$, $k = 1, \ldots, m$, be the APR given by DM e_k at the CEP round t. The competence of DM e_k is

$$\psi\left(P^{(k,t)}\right) = \frac{1}{6}\sum_{i=1}^{n}\sum_{j=1}^{n}\psi_{ij} \tag{17}$$

where ψ_{ij} is computed with Algorithm 2 of the ordinal consistency detection process in [19]. A large value of $\psi(P^{(k,t)})$ means a poor credibility of DM e_k, and the probability of being blindly trusted increases. If $\psi(P^{(k,t)}) = 0$, DM e_k is trustworthy. If $\psi(P^{(k,t)}) > 0$, the third party concludes that DM e_k satisfies trust risks induced by Factor I at CEP round t.

2) Factor II (Consistency): Consistency indicates the level of cognition and knowledge of DMs, which reflects their trustworthiness in a group. Multiplicative consistency is an appropriate property for examining DMs' cognition and knowledge. In SNGDM, if a DM with a low level of cognition and knowledge is given an unreasonable TD by others, a biased and misleading decision may occur.

By (2), the multiplicative consistency level GCI of $P^{(k,t)}$ is calculated. The smaller the GCI$(P^{(k,t)})$ value, the more trustworthy the DM e_k will be. Given the GCI thresholds of Table I, if GCI$(P^{(k,t)}) > \overline{\text{GCI}}$, the third party deduces that DM e_k meets the cognition and knowledge trust risk problem induced by Factor II at CEP round t. This may create a situation where a DM without acceptable multiplicative consistency is blindly or over-trusted.

3) Factor III (Integrity): The integrity of DMs reflects whether they can honestly express their opinions. In CEP, some DMs may deliberately conceal true information and display dishonest preferences to achieve their own benefit. A DM with low degree of honesty but high trust value in CEP is at risk of being blindly trusted.

Khalid and Beg [25] studied the role of honesty in decision making and suggested that the level of honesty can be derived from the average fuzziness of the DM's APR. They argue that the closer a DM's preference values are to 0.5, the stronger the ambiguity of such preferences, and the more dishonest the DM. The average fuzziness $\overline{H}$ of APR $P^{(k,t)}$ is defined as the [0, 1] value [25]

$$\bar{H}\left(P^{(k,t)}\right) = \frac{2}{n(n-1)}\sum_{i=1}^{n-1}\sum_{j=i+1}^{n} H\left(p_{ij}^{(k,t)}\right) \tag{18}$$

where

$$H\left(p_{ij}^{(k,t)}\right) = \begin{cases} \frac{p_{ij}^{(k,t)}}{0.5-\varepsilon^{(t)}}, & p_{ij}^{(k,t)} \in \left[0, 0.5-\varepsilon^{(t)}\right) \\ 1, & p_{ij}^{(k,t)} \in \left[0.5-\varepsilon^{(t)}, 0.5+\varepsilon^{(t)}\right] \\ \frac{p_{ij}^{(k,t)}-1}{\varepsilon^{(t)}-0.5}, & p_{ij}^{(k,t)} \in \left(0.5+\varepsilon^{(t)}, 1\right] \end{cases} \tag{19}$$

and

$$\varepsilon^{(t)} = \frac{2}{mn(n-1)}\sum_{k=1}^{m}\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\left|p_{ij}^{(k,t)} - 0.5\right| \tag{20}$$

is the average deviation of all preference values from 0.5.

A small value of $\overline{H}(P^{(k,t)})$ implies a high honesty degree of DM e_k. Given a threshold value $\alpha(\alpha \in [0,\ 1])$, if $\overline{H}(P^{(k,t)}) \geq \alpha$, then the third party infers that DM e_k has a low degree of honesty and at risk of being endowed with excessive trust due to Factor III at CEP round t.

4) Factor IV (Fairness): Fairness is a condition of trust, which shows the DMs' resistance to external temptations and ensures that DMs give their preferences impartially. DMs who express their views in a biased or unfair way may mislead others in a group. If a DM with poor fairness is given a high weight during the aggregation process, she/he is at risk of being blindly trusted.

The consensus reaching process essentially follows the majority principle. If the best choice of an individual DM's preference ordering is different from that of the collective preference ordering, there is a risk of such DM of being tempted by the outside world. Denoting by $V^{(c,t)} = (v_1^{(c,t)}, \ldots, v_n^{(c,t)})^T$ and $V^{(k,t)} = (v_1^{(k,t)}, \ldots, v_n^{(k,t)})^T$, $k = 1, \ldots, m$, the preference vectors of the alternatives from the collective APR $P^{(c,t)}$ and the individual APR $P^{(k,t)}$, computed by (4), respectively, at the round t, and $o : \{1, \ldots, n\} \to \{1, \ldots, n\}$ being the permutation such that $v_{o(i)} \geq v_{o(i+1)}$, for all $i = 1, \ldots, n-1$, where $v_{o(i)}$ is the ith largest value in the set of $\{v_1, \ldots, v_n\}$, then the preference orderings of alternatives from collective and individual APRs are $O(V^{(c,t)}) = (o^{(c,t)}(1), \ldots, o^{(c,t)}(n))^T$ and $O(V^{(k,t)}) = (o^{(k,t)}(1), \ldots, o^{(k,t)}(n))^T$, respectively. Therefore, the 0-1 variable

$$s^{(k,t)} = \begin{cases} 1, & o^{(c,t)}(1) \neq o^{(k,t)}(1) \\ 0, & o^{(c,t)}(1) = o^{(k,t)}(1) \end{cases} \tag{21}$$

can be used by the third party to conclude that DM e_k satisfies the characteristic of trust risk problem generated by Factor IV in the CEP round t when $s^{(k,t)} = 1$.

5) Factor V (Receptivity): Receptivity indicates the degree of harmony and agreement of different opinions among DMs. CEP is a process of eliminating conflicts between DMs and consolidating their views. The receptivity of a DM can be measured by the existent gap between her/his views and the views of others. In CEP, when the opinion of a DM is quite different from that of others, then her/his receptivity is considered quite poor. Moreover, if she/he is trusted by other DMs, the DM may pose a risk of misleading the public. The following value in [0, 1] is therefore proposed to measure the deviation of DM e_k with the rest of DMs:

$$r^{(k,t)} = \frac{2}{(m-1)n(n-1)} \sum_{h=1,h\neq k}^{m} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \left| p_{ij}^{(k,t)} - p_{ij}^{(h,t)} \right|. \quad (22)$$

Given a threshold $\beta(\beta \in [0,\ 1])$, if $r^{(k,t)} \geq \beta$, the third party infers that DM e_k satisfies the trust risks induced by Factor V at CEP round t.

Factors I–V are based on the preferences given by DMs and are the criteria for third party to objectively evaluate DMs' credibility. Correspondingly, a third-party OEM can be established which contains five attributes: 1) competence (c_1); 2) consistency (c_2); 3) integrity (c_3); 4) fairness (c_4); and 5) receptivity (c_5). The factors that cause trust risks in real SNGDM scenarios are different, so, at each CEP round, the third party monitors the performance of DMs to infer the potential risk-inducing factors, and the assessment of the corresponding attributes of DMs in the OEM are dynamically updated. DMs' credibility weights are calculated as per $(M-1)$.

Trust relationships of DMs described by the SN structure reflect the prestige and importance of DMs in a group. Also, it is a factor that affects trust in SNGDM. Combining TDs derived from the SN structure with the attributes of OEM, an MTAM can be logically constructed based on the following six attributes: 1) competence (c_1); 2) consistency (c_2); 3) integrity (c_3); 4) fairness (c_4); 5) receptivity (c_5); and 6) SN structure (c_6). The attributes of this MTAM are comprehensive and allow to determine the DMs' weights in CEP. Similarly, the values of each attribute in the MTAM can be dynamically updated as per the objective evaluation information of the third party.

Based on the third-party evaluation information, a trust risk measurement method is proposed, which is based on monitoring the deviation between the DMs' credibility ranking (from the OEM) and the DMs' aggregation weight ranking (from the MTAM). Denoting by $\mathrm{OEM}^{(t)}$ and $\mathrm{T}^{(t)}$ the evaluation matrices given by the third party at CEP round t, as per $(M-1)$, the DMs' weights, denoted $\lambda(\mathrm{OEM}^{(t)})$ and $\lambda(\mathrm{T}^{(t)})$, respectively, are calculated. Let $o^{(\mathrm{OEM},t)}(i)$ and $o^{(T,t)}(i)$ be the positions of the ith largest element in $\lambda(\mathrm{OEM}^{(t)})$ and $\lambda(\mathrm{T}^{(t)})$, respectively. Then, $O(\lambda(\mathrm{OEM}^{(t)})) = (o^{(\mathrm{OEM},t)}(1), \ldots, o^{(\mathrm{OEM},t)}(m))^T$ and $O(\lambda(\mathrm{T}^{(t)})) = (o^{(T,t)}(1), \ldots, o^{(T,t)}(m))^T$ are the ranking of $\lambda(\mathrm{OEM}^{(t)})$ and $\lambda(\mathrm{T}^{(t)})$, respectively.

The blind trust and lack of trust for a DM can be detected and defined as follows.

Definition 8: DM $e_{o^{(\mathrm{OEM},t)}(k)}$ is at risk of being blindly trusted at CEP round t, if

$$\sigma^{(\mathrm{OEM},t)}\left(o^{(\mathrm{OEM},t)}(k)\right) - \sigma^{(T,t)}\left(o^{(\mathrm{OEM},t)}(k)\right) > 0 \quad (23)$$

where $\sigma^{(\mathrm{OEM},t)}(o^{(\mathrm{OEM},t)}(k))$ and $\sigma^{(T,t)}(o^{(\mathrm{OEM},t)}(k))$ are the rank positions of the $o^{(\mathrm{OEM},t)}(k)$ for $O(\lambda(\mathrm{OEM}^{(t)}))$ and $O(\lambda(\mathrm{T}^{(t)}))$, respectively. Conversely, DM $e_{o^{(\mathrm{OEM},t)}(k)}$ is at risk of lacking reasonable trust at CEP round t, if

$$\sigma^{(\mathrm{OEM},t)}\left(o^{(\mathrm{OEM},t)}(k)\right) - \sigma^{(T,t)}\left(o^{(\mathrm{OEM},t)}(k)\right) < 0. \quad (24)$$

The absolute value of the above deviations is proposed to measure the trust risk degree of DM $e_{o^{(OEM,t)}(k)}$ at CEP round t

$$\phi\left(e_{o^{(\mathrm{OEM},t)}(k)}\right) = \left|\sigma^{(\mathrm{OEM},t)}\left(o^{(\mathrm{OEM},t)}(k)\right) - \sigma^{(T,t)}\left(o^{(\mathrm{OEM},t)}(k)\right)\right|. \quad (25)$$

Definition 9: The group TRI in [0, 1] of CEP round t is

$$\mathrm{TRI}^{(t)} = \begin{cases} \frac{2}{(m-1)(m+1)} \sum_{k=1}^{m} \phi\left(e_{o^{(\mathrm{OEM},t)}(k)}\right), & m \text{ is odd} \\ \frac{2}{m^2} \sum_{k=1}^{m} \phi\left(e_{o^{(\mathrm{OEM},t)}(k)}\right), & m \text{ is even.} \end{cases} \quad (26)$$

It is unrealistic to have no risk in real-world SNGDM. Therefore, in the decision-making process, it is reasonable for the third party to set an acceptable risk index threshold $\overline{\mathrm{TRI}}$. If $\mathrm{TRI}^{(t)} < \overline{\mathrm{TRI}}$, the acceptable trust risk of SNGDM is realized; otherwise, the following trust risk dynamic management mechanism is activated.

C. Trust Risk Dynamic Management Mechanism

In order to achieve acceptable group TRI, this section designs a dynamic third-party trust risk management mechanism. The role of the third-party agency is important. On the one hand, the third-party organization uses different management measures to update the MTAM for DMs' different trust risk types. Setting the evaluation values of these attributes dynamically in MTAM is equivalent to effectively managing trust risks. On the other hand, the third-party organization encourages the high-risk DMs to modify their preference information. Considering the DMs' credibility, the recommended modification may be more acceptable for the DM if it comes from the DM with highest credibility. Specifically, the trust risk dynamic management mechanism includes the following two phases.

1) *Identification of the DM With Highest Trust Risk Level:* This DM has the greatest impact on the reliability of group's views because her/his preference information has a negative impact on CEP and misleads the decision results. Thus, the DM e_k with the maximum value of ϕ_k is suggested to modify her/his information at each round of management mechanism.
2) *Adjustment Process:* As per Definition 8, the trust risk type of the identified DM e_k in phase 1) is determined. For each of two trust risk type in Definition 8, the third party proceeds differently as follows.
    a) If DM e_k lacks reasonable trust, the attributes evaluation for DM e_k in the MTAM will be increased as compensation and reward.

b) If DM e_k is blindly trusted, the corresponding attribute evaluation in the MTAM will be updated as punishment, in addition to the modification of her/his APR, $P^{(k)}$, into the following APR $\bar{P}^{(k)} = (\bar{p}_{ij}^{(k)})_{n\times n}$:

$$\begin{cases} \bar{p}_{ij}^{(k)} = (1-\xi)p_{ij}^{(k)} + \xi p_{ij}^{(h)}, & i \le j, k = 1, \ldots, m \\ & 0 \le \xi \le 1 \\ \bar{p}_{ji}^{(k)} = 1 - \bar{p}_{ij}^{(k)}, & i > j \end{cases} \tag{27}$$

where $P^{(h)}$ is the APR provided by the most credible DM, that is, the DM with lowest trust risk level.

Remark 2: The proposed trust risk management mechanism is automatic. As mentioned in Remark 1, there may also be an extreme case in phase 2) where the DM with highest trust risk level is unwilling to modify her/his APR based on the third-party opinions. This behavior is of no benefit to trust risk management. A DM unwilling to accept the third-party's strong recommendation, but receptable to change, is allowed to adjust the APR voluntarily. If the ϕ_k of the new APR is lower than its current value, the new APR is effective. For a DM unwilling to change preferences, her/his APR is discarded in SNGDM.

IV. Simulation Experiments and Discussions

This section contains a detailed simulation methodology (Section IV-A) and analyzes the experimental results obtained by the developed simulation methodology regarding their support toward the feasibility and validity of the proposed CEP framework (Sections IV-B, IV-C, and IV-D). Section IV-E discusses the applicability of the proposed decision aid model in real world, including the practical meaning and collection methods of the model input information.

A. Simulation Methodology

The proposed simulation methodology is based on the random generation of the initial APRs and SN-based TDs of DMs in [0, 1]. The first five attributes' values of the initial MTAM are all set to 100, while the values of attribute c_6 are determined by the SN structure. Based on Hypotheses 1 and 2, a third party supervises DMs' performance to detect and regulate the trust risk issues in CEP, thereby reducing TRI and reaching a consensus as proposed in Section III. The algorithmic form of the proposed simulation methodology is given in Algorithm 1.

Algorithm 1 Simulation Algorithm of CEP Framework Under Trust Risk Problems

Input: number of DMs, m; number of alternatives, n; threshold for GCI, $\overline{\text{GCI}}$; threshold of integrity degree, α; threshold of receptivity, β; threshold of TRI, $\overline{\text{TRI}}$; threshold of group conflict level, δ; reward and penalty coefficient, χ; modification and fusion coefficient, ξ; and maximum iteration number, $t_{\max}$.
Output: group conflict level, $\theta^{(c)}$; TRI; number of iterations, t; and ranking result.
Step 1: Randomly construct m $n\times n$ APRs, $\{P^{(1)}, \ldots, P^{(m)}\}$, and TDs derived by the SN structure.
Step 2: Let $t = 0$, $P^{(k,t)} = P^{(k)}$, $k = 1, \ldots, m$.
Step 3: Construct MTAM $T^{(t)} = (t_{kj}^{(t)})_{m\times l}$. Apply (10) to compute the DMs' weighting vectors.
Step 4: Based on Factors I–V, the third party supervise the DMs' performance in CEP. The OEM$^{(t)}$ is yielded by the following two cases.
A. If $t = 0$

$$OEM^{(t)} = (t_{kj}^{(t)})_{m\times(l-1)},$$
$$t_{kj}^{(t)} = \begin{cases} 100 - 100\chi, & \text{if DM } e_k \text{is in ferred to have a blind trust problem caused by attribute } j \\ 100, & \text{if DM} e_k \text{has no trust risk issues} \end{cases} \tag{28}$$

B. If $t \ge 1$

$$OEM^{(t)} = (t_{kj}^{(t)})_{m\times(l-1)},$$
$$t_{kj}^{(t)} = \begin{cases} t_{kj}^{(t-1)} - 100\chi, & \text{if DM} e_k \text{is inferred to have a blind trust problem caused by attribute } j \\ t_{kj}^{(t-1)}, & \text{if DM} e_k \text{has no trust risk issues} \end{cases} \tag{29}$$

Then, apply (10) to calculate the weights of DMs' credibility.
Step 5: Apply (25) and (26) to compute the group trust risk level, TRI$^{(t)}$. If TRI$^{(t)} < \overline{\text{TRI}}$ or $t \ge t_{\max}$, then go to step 7; otherwise, continue to the next step.
Step 6: Update MTAM $T^{(t+1)} = (t_{kj}^{(t+1)})_{m\times l}$ based on OEM$^{(t)}$. According to (25), identify the DM e_k with the highest trust risk level and judge the type of trust risk she/he exhibits as per Definition 8. Without loss of generality, the treatment for DM e_k is as follows.
A. If DM e_k is blindly trusted, she/he is encouraged to provide $P^{(k,t+1)}$ using (27); t=t+1 and go to step 3.
B. If DM e_k lacks sufficient trust, OEM$^{(t)}$ needs to be further refreshed as

$$OEM^{(t+1)} = (t_{kj}^{(t+1)})_{m\times(l-1)},$$
$$t_{kj}^{(t+1)} = \begin{cases} t_{kj}^{(t)} + 100\chi, & \text{if DM } e_k \text{is inferred to lack sufficient trust, } j = 1, \ldots, l-1 \\ t_{kj}^{(t)}, & \text{if DM } e_k \text{has no trust risk issues} \end{cases} \tag{30}$$

$t = t + 1$ and go to step 5.
Step 7: Obtain the final updated MTAM T$^{(t)}$ as per OEM$^{(t)}$, and derive the reasonable aggregation weights of DMs from MTAM by (10).
Step 8: Utilize (15) to calculate the group conflict level, $\theta^{(c,t)}$. If $\theta^{(c,t)} \le \delta$ or $t \ge t_{\max}$, then go to step 10; otherwise, move on to the next step.
Step 9: Identify the DM e_k with highest conflict level. Encourage DM e_k to modify her/his APR using (16).
Step 10: Rank the alternatives by (4). Output $\theta^{(c)}$; TRI; t.

B. Experimental Results (The Impact of the Threshold $\overline{TRI}$)

The experimental settings based on the above simulation methodology are: $t_{\max} = 5$, $\delta = 0.25$, $\alpha = 0.9$, $\beta = 0.35$, $\chi = 0.15$, and $\xi = 0.5$. Constructing different input parameters m, n, and $\overline{\text{TRI}}$, the simulation experiment is run 1000 times to calculate average values of TRI, $\theta^{(c)}$, t, etc.

To explain the effectiveness of the proposed trust risk dynamic management mechanism, the trust risk mitigation degree (TRMD) and the decrement ratio (DR) for the risky DMs are recorded. Let TRI$^{(0)}$ and TRI* be the group trust risk level at the initial state and the final state, respectively. The number of DMs with trust risk at the initial state and the final state after mitigating the group TRI are denoted by r and r', respectively. The TRMD and DR are defined as

$$\text{TRMD} = \text{TRI}^{(0)} - \text{TRI}^* \tag{31}$$

$$\text{DR} = \frac{r}{m} - \frac{r'}{m}. \tag{32}$$

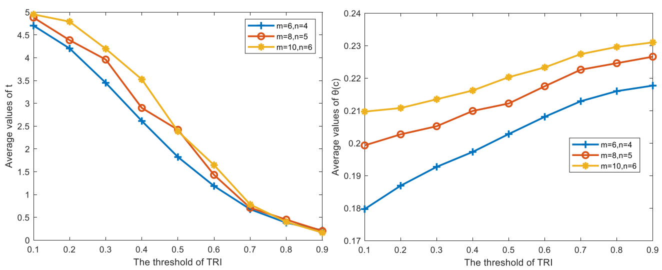
The experimental results, based on the given SN structure in Example 1 and a random SN structure, are listed in Tables III and IV. Furthermore, the average values of t and $\theta^{(c)}$ in the simulation methodology under different values of parameter $\overline{\text{TRI}}$ are depicted in Fig. 4. The following three observations can be drawn.

TABLE III
EFFECT OF DIFFERENT $\overline{\text{TRI}}$ ON THE SIMULATION RESULTS UNDER THE GIVEN SN STRUCTURE IN EXAMPLE I

m	n	$\overline{TRI}$	Average value of TRI	TRMD	r	r'	DR	Mean value of t	Average value of $\theta^{(c)}$
5	4	0.3	0.1265	49.10%	3.8620	1.4590	48.06%	2.3630	0.1838
		0.5	0.2602	35.73%	3.8620	2.4810	27.62%	1.4270	0.1923
	6	0.3	0.1617	38.53%	3.5450	1.7200	36.50%	2.5840	0.1885
		0.5	0.2700	27.70%	3.5450	2.4340	22.22%	1.3540	0.1978

TABLE IV
INFLUENCE OF DIFFERENT $\overline{\text{TRI}}$ ON THE SIMULATION RESULTS UNDER THE RANDOM SN STRUCTURE

m	n	$\overline{TRI}$	Average value of TRI	TRMD	r	r'	DR	Mean value of t	Average value of $\theta^{(c)}$
5	4	0.3	0.1840	46.72%	3.9380	1.9470	39.82%	3.3730	0.1798
		0.5	0.2825	36.87%	3.9380	2.7210	24.34%	2.3870	0.1883
	6	0.3	0.2015	45.07%	3.9360	2.0260	38.20%	3.5510	0.1846
		0.5	0.2905	36.17%	3.9360	2.6990	24.74%	2.4980	0.1923
7	4	0.3	0.2428	42.59%	5.9770	4.1440	26.19%	3.6490	0.1984
		0.5	0.3614	30.73%	5.9770	5.0480	13.27%	2.3720	0.2061
	6	0.3	0.2624	39.97%	5.9850	4.2880	24.24%	3.8410	0.1998
		0.5	0.3715	29.06%	5.9850	5.1050	12.57%	2.4990	0.2073
9	4	0.3	0.2676	39.76%	8.0070	6.2250	19.80%	4.0860	0.2077
		0.5	0.3979	10.03%	8.0070	7.1040	26.72%	2.3990	0.2142
	6	0.3	0.2885	37.55%	7.9310	6.3830	17.20%	4.2720	0.2108
		0.5	0.4021	26.19%	7.9310	7.1850	8.29%	2.6300	0.2174



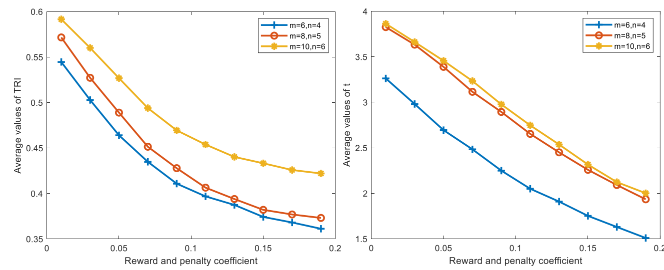
(a) (b)

Fig. 4. Average values of t and $\theta^{(c)}$ under different parameter $\overline{\text{TRI}}$: (a) $\overline{\text{TRI}}$ versus t and (b) $\overline{\text{TRI}}$ versus $\theta^{(c)}$.

1) Tables III and IV reveal that the trust risk issues of SNGDM are widespread. At the same time, they also show that the proposed approach can effectively control the number of DMs with trust risks within a group. As per the experimental results, at the initial stage $r \neq 0$, which indicates that DMs with trust risks are widely distributed. The larger the number of DMs in a group, the greater the number of risky DMs. However, through the dynamic supervision of the third-party agency, the number of risky DMs is significantly reduced. Therefore, to ensure the rationality of the final decision, it is effective and necessary for a third party to monitor and manage the trust risks in SNGDM.
2) The conflict resolution framework can effectively manage trust risk issues for different parameter values of $\overline{\text{TRI}}$, and it can simultaneously realize the dynamic trust risk management and consensus. Overall, in Tables III and IV, TRMD is large, and the average value of TRI is significantly reduced to an acceptable range. In most cases, it takes 2–3 rounds on average to reach an acceptable level of trust risk and consensus, and the success rate is very high.
3) Fixing m and n, as the TRI threshold value decreases, the average value for $\theta^{(c)}$ decreases, while the average value of t increases. It means that the adoption of undemanding standards to manage trust risk issues will achieve the group's acceptable risk level faster, and speed up consensus.

TABLE V
INFLUENCE OF DIFFERENT PARAMETER, χ, ON THE EXPERIMENTAL RESULTS UNDER A RANDOM SN STRUCTURE

m	n	χ	Average value of TRI	TRMD	Mean value of t	Average value of $\theta^{(c)}$
5	4	0.05	0.4137	23.78%	3.2880	0.1893
		0.1	0.3220	32.95%	2.7540	0.1881
		0.15	0.2812	37.03%	2.3190	0.1885
	6	0.05	0.4315	22.33%	3.3430	0.1921
		0.1	0.3390	31.58%	2.8600	0.1919
		0.15	0.2878	36.70%	2.4660	0.1924
7	4	0.05	0.4838	18.72%	3.5070	0.2028
		0.1	0.3979	27.31%	2.8840	0.2028
		0.15	0.3647	30.63%	2.3470	0.2036
	6	0.05	0.4788	17.67%	3.4400	0.2074
		0.1	0.4024	25.30%	2.8960	0.2072
		0.15	0.3728	28.26%	2.4240	0.2079
9	4	0.05	0.5112	14.98%	3.6570	0.2140
		0.1	0.4298	23.12%	3.0220	0.2137
		0.15	0.3994	26.16%	2.4350	0.2146
	6	0.05	0.5137	13.85%	3.6350	0.2168
		0.1	0.4401	21.21%	3.0720	0.2165
		0.15	0.4057	24.65%	2.5860	0.2170



(a) (b)

Fig. 5. Average values of TRI and t under different parameter χ: (a) χ versus TRI and (b) χ versus t.

C. Experimental Results (The Influence of the Reward and Penalty Coefficient χ)

Similar settings to those used in Section IV-B are used in this case: $t_{\max} = 5$, $\delta = 0.25$, $\alpha = 0.9$, $\beta = 0.35$, $\xi = 0.5$, and $\overline{\text{TRI}} = 0.5$. Setting different input parameters m, n, and χ, the simulation experiment is run 1000 times to obtain average values of TRI, $\theta^{(c)}$, t, and TRMD. The experimental results in Table V are based on a random SN structure. Moreover, the average values of TRI and t in the simulation experiment under different values of the parameter χ are depicted in Fig. 5. It can be seen that when m and n are fixed, the increase of the reward and punishment coefficient χ translates into a decrease of the average values of TRI and t. If the reward and penalty coefficient χ is too small, then the TRI cannot be effectively alleviated. This finding implies that the appropriate use of strong reward and penalty coefficient to manage the trust risk issues can accelerate the mitigation of trust risk levels, increase the success rate of trust risk control, and speed up consensus.

D. Experimental Results (Our Framework Versus Traditional CEP)

Herein, to verify the validity and applicability of the proposed CEP under trust risk issues, it is compared with the

TABLE VI
COMPARISON RESULTS BETWEEN OUR PROPOSED METHOD AND TRADITIONAL CEP UNDER THE GIVEN SN STRUCTURE IN EXAMPLE I

Method	m	n	Average value of *TRI*	TRMD	r	r'	DR	Mean value of t	Average value of $\theta^{(c)}$
Our proposal	5	4	0.2503	36.17%	3.8180	2.3820	28.72%	1.3930	0.1950
		6	0.2717	28.88%	3.6700	2.5070	23.26%	1.3920	0.1979
Traditional CEP	5	4	0.5962	1.58%	3.8180	3.7980	0.4%	1.4920	0.2108
		6	0.5227	3.78%	3.6700	3.5550	2.30%	1.4120	0.2141

TABLE VII
COMPARISON RESULTS BETWEEN OUR PROPOSED METHOD AND TRADITIONAL CEP UNDER THE RANDOM SN STRUCTURE

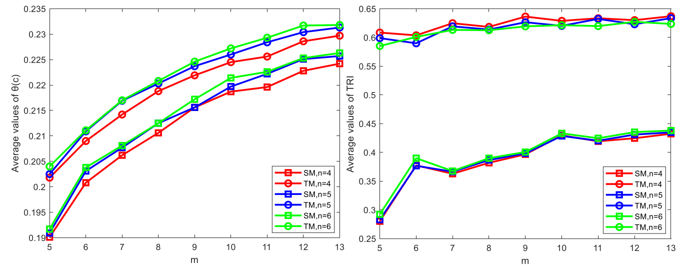
Method	m	n	Average value of *TRI*	TRMD	r	r'	DR	Mean value of t	Average value of $\theta^{(c)}$
Our proposal	5	4	0.2875	36.22%	3.9570	2.7550	24.04%	2.2140	0.1898
		6	0.2965	35.02%	3.9230	2.7840	22.78%	2.4720	0.1921
	7	4	0.3651	29.14%	5.9640	5.0810	12.61%	2.3610	0.2066
		6	0.3645	29.00%	5.9340	5.0700	12.34%	2.4380	0.2072
	9	4	0.3978	25.53%	7.9610	7.2010	8.44%	2.3670	0.2157
		6	0.4031	25.66%	7.9700	7.1200	9.44%	2.5890	0.2166
Traditional CEP	5	4	0.6103	3.93%	3.9570	3.8790	1.56%	2.3040	0.2025
		6	0.5942	5.25%	3.9230	3.8000	2.46%	2.4850	0.2033
	7	4	0.6268	2.98%	5.9640	5.9270	0.53%	2.4730	0.2163
		6	0.6122	4.23%	5.9340	5.8490	1.21%	2.4620	0.2168
	9	4	0.6279	2.52%	7.9610	7.9080	0.59%	2.5050	0.2230
		6	0.6227	3.70%	7.9700	7.8970	0.81%	2.6220	0.2250

traditional CEP from two aspects: 1) performance analysis and 2) complexity analysis.

1) Performance Analysis: In traditional CEP, DMs' weights are determined by the trust relationship described by SN structure, and usually remain unchanged throughout the entire process. Consequently, in the simulation experiment, the corresponding traditional CEP can be obtained from the proposed approach by suppressing the dynamic weight generation process and trust risk dynamic management steps. Thus, the removal of steps 3–7 from Section IV-A simulation methodology corresponds to the simulation methodology of the traditional CEP.

From a performance point of view, the traditional CEP ignores the trust risk issues and the dynamic changes of DMs' weights in SNGDM, while our developed decision framework sets up the trust risk measurement and dynamic management mechanism to solve these problems. In general, the proposed model has more functions and better performance than the traditional consensus. In what follows, a visual comparison of the performance of these two methods by means of the simulation experiment is provided. Like in Sections IV-B and IV-C, the experiment settings are: $t_{\max}$=5, $\delta = 0.25$, $\alpha = 0.9$, $\beta = 0.35$, $\xi = 0.5$, $\chi = 0.15$, and $\overline{\mathrm{TRI}} = 0.5$. Setting different input parameters m and n, the simulation experiments for the proposed CEP and the traditional CEP are run 1000 times to compute average values of TRI, $\theta^{(c)}$, t, etc. The results based on the SN structure of Example 1 and a random SN structure are shown in Tables VI and VII. Also, the average values of $\theta^{(c)}$ and TRI under different parameters are depicted in Fig. 6. In these figures, the proposed method is denoted as SM, and the traditional method is denoted as TM. The following two observations are drawn.

1) From Fig. 6(a), the proposed framework can accelerate consensus while managing trust risks. For different m, the value of $\theta^{(c)}$ obtained with the proposed method is smaller than that of the traditional CEP, indicating that the consensus level of the proposed CEP is significantly better than that of traditional CEP. In summary, the success rate of conflict elimination improves with the proposed method, which also supports dynamically regulation of the trust risk issues in SNGDM.
2) From Fig. 6(b), traditional CEP usually has a high TRI, so trust risk problems often exist in CEP and it is given the consideration it deserves. In comparison with traditional CEP, the proposed CEP can eliminate the conflicts between DMs' opinions, alleviate group TRI and avoid blind trust or lack of due trust of DMs. Thus, it is found that the proposed CEP can control TRI and reduce the number of DMs with trust risks in a group, which endorses the credibility and reliability of the final decision results.



(a) (b)

Fig. 6. Average values of $\theta^{(c)}$ and TRI for the proposed CEP and traditional CEP: (a) m versus $\theta^{(c)}$ and (b) m versus TRI.

TABLE VIII
TIME COMPLEXITY COMPARISON BETWEEN THE PROPOSED CEP AND TRADITIONAL CEP

n	The proposed CEP	The traditional CEP
4	0.00619s	0.00028s
5	0.00754s	0.00035s
6	0.00872s	0.00038s
7	0.01225s	0.00051s
8	0.01390s	0.00055s
9	0.01601s	0.00063s

2) Complexity Analysis: The proposed CEP has more steps than traditional CEP, since it has to realize the measurement and management of trust risk and the dynamic derivation of weights. From the perspective of the algorithm steps, the proposed method looks more complicated, although its logic well-grounded since it is able to perform sensible tasks that cannot be achieved by the traditional CEP. With a group of five DMs as an example, the time complexity of the two compared methods to obtain the ranking result is shown in Table VIII. It can be observed that there is not much difference on operation time between the two methods, requiring slightly more time the proposed method due to its extra steps. Thus, it can be said that in generally, the proposed method shows feasibility and validity with regards to time complexity.

The number of iterations required by different algorithms to achieve their goals also reflects their computational complexity. Through simulation experiments, it is found that the average number of iterations required by the proposed approach to reach consensus is lower than the traditional CEP (Tables VI and VII). Similar to the previous simulation experiment, the simulation experiments for the proposed CEP and the traditional CEP are run 1000 times to compute average

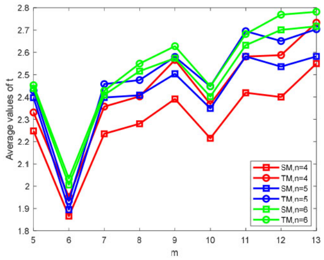


Fig. 7. Average values of t for the proposed CEP and traditional CEP.

values of t. The average values of t under different input parameters, m and n, are shown in Fig. 7. From Fig. 7, for a given m and n, the average number of consensus rounds in the proposed CEP framework is consistently lower than the traditional CEP. Usually, it takes 2–3 rounds on average to reach an acceptable level of trust risk and consensus, and the success rate is very high. Thus, the proposed framework significantly accelerates consensus, and reduces the consensus costs, when compared with the traditional framework.

E. Discussion

In order to ensure the applicability of the proposed decision aid model in the real world, the practical meaning and the collection methods of the input information for this model are analyzed.

For a practical SNGDM problem, m DMs give their opinions on n alternatives to a decision problem on the SN platform to find the collective optimal solution. DMs express their opinions through pairwise comparisons of alternatives, which is mathematically modeled as APRs [19]. In view of the widespread trust risk problems in SNGDM, to alleviate the level of trust risk and improve the credibility and reliability of decision results, the proposed decision aid model is adopted to help DMs make decision.

To ensure the smooth progress of the model, it is necessary to explain the meaning and use of the parameters required in the model and give suggestions for all DMs before making a decision. In credibility assessment, $\overline{\mathrm{GCI}}$ is the consistency threshold widely used by DMs (Table I): it takes different values for different values of parameter n, and does not need to be set by DMs. Integrity threshold α is used to measure whether DMs have acceptable honesty. Complete honesty is difficult to achieve in practice. The smaller the threshold α is set, the harder it is for DMs to meet this requirement. Therefore, implementing a less stringent threshold for the evaluation of this criterion would be easier to be accepted by DMs. For example, the threshold range is set in [0.75, 0.95]. Receptivity threshold β is utilized to measure the gap between two DMs' opinions. The smaller the difference between a DM and others, the higher the credibility. In reality, due to different knowledge backgrounds or interest of DMs, differences in opinions are normal, and the threshold β can be set to a more relaxed interval [0.15, 0.45]. In CEP, $\overline{\mathrm{TRI}} \in [0,\ 1]$ and it is the maximum trust risk level that group can bear. Risks are always involved in decision making, so completely risk-free is difficult to achieve in real world. Consequently, it is more acceptable for all DMs to implement in the model a relatively strict $\overline{\mathrm{TRI}}$. Generally, $\overline{\mathrm{TRI}}$ is set in [0.2, 0.5]. $\delta \in [0, 1]$ and it is the maximum group conflict level. A value $\delta = 0$ is an unlikely scenario for a group, and a soft consensus is adopted, that is, $\delta \in [0.05, 0.35]$. The stringency of $\overline{\mathrm{TRI}}$ and δ directly affects the number of iterations. Thus, the stricter these thresholds are set, the more iterations are required to achieve the goal. ξ is a modification and fusion coefficient measured in [0, 1]. To maintain neutrality, the value $\xi = 0.5$ is always been selected. Reward and punishment coefficient χ is related to the maximum number of iterations $t_{\max}$ as follows $t_{\max} = \lfloor 100/\chi \rfloor$. Hence, increasing χ reduces, in general, the number of iterations required.

On the premise that DMs fully understand these parameters, as per their willingness, the thresholds are given and fed back to the third party, and then the decision aid model is activated.

V. Illustrative Example

This section reports an example illustrating how the proposed trust risk analysis-based CEP for SNGDM works. Let $E = \{e_1, \ldots, e_5\}$ be the set of five DMs in Fig. 2, and their APRs on a set of four alternatives $X = \{x_1, \ldots, x_4\}$ being the following:

$$P^{(1)} = P^{(1,0)} = \begin{pmatrix} 0.5 & 0.4 & 0.7 & 0.5 \\ 0.6 & 0.5 & 0.8 & 0.6 \\ 0.3 & 0.2 & 0.5 & 0.3 \\ 0.5 & 0.4 & 0.7 & 0.5 \end{pmatrix}$$

$$P^{(2)} = P^{(2,0)} = \begin{pmatrix} 0.5 & 0.25 & 0.15 & 0.65 \\ 0.75 & 0.5 & 0.6 & 0.8 \\ 0.85 & 0.4 & 0.5 & 0.6 \\ 0.35 & 0.2 & 0.4 & 0.5 \end{pmatrix}$$

$$P^{(3)} = P^{(3,0)} = \begin{pmatrix} 0.5 & 0.3 & 0.6 & 0.7 \\ 0.7 & 0.5 & 0.1 & 0.3 \\ 0.4 & 0.9 & 0.5 & 0.7 \\ 0.3 & 0.7 & 0.3 & 0.5 \end{pmatrix}$$

$$P^{(4)} = P^{(4,0)} = \begin{pmatrix} 0.5 & 0.7 & 0.9 & 0.5 \\ 0.3 & 0.5 & 0.6 & 0.7 \\ 0.1 & 0.4 & 0.5 & 0.8 \\ 0.5 & 0.3 & 0.2 & 0.5 \end{pmatrix}$$

$$P^{(5)} = P^{(5,0)} = \begin{pmatrix} 0.5 & 0.2 & 0.6 & 0.4 \\ 0.8 & 0.5 & 0.9 & 0.7 \\ 0.4 & 0.1 & 0.5 & 0.3 \\ 0.6 & 0.3 & 0.7 & 0.5 \end{pmatrix}.$$

As per the previous section and the DMs' willingness, the relevant selected thresholds are: $\overline{\mathrm{GCI}} = 0.3526$, $\alpha = 0.9$, $\beta = 0.35$, $\xi = 0.5$, $\delta = 0.25$, $\chi = 0.15$, and $\overline{\mathrm{TRI}} = 0.5$. The OWA operator with linguistic quantifier "most" is implemented. In addition, it is assumed that MTAM with six attributes: 1) competence (c_1); 2) consistency (c_2); 3) integrity (c_3); 4) fairness (c_4); 5) receptivity (c_5); and 6) SN structure (c_6), has original values of 100 for the first five attributes, while the values of attribute c_6 are derived from SN structure. Meanwhile, we assume that the weighs of attributes in MTAM and OEM are equal. From Example 1, $\mathrm{TD}(e_1) = 0.41$, $\mathrm{TD}(e_2) = 0.46$, $\mathrm{TD}(e_3) = 0.63$, $\mathrm{TD}(e_4) = 0.38$, and TD(e_5) = 0.36. Therefore, the initial MTAM $T^{(0)}$ is

$$T^{(0)} = \begin{pmatrix} 100 & 100 & 100 & 100 & 100 & 0.41 \\ 100 & 100 & 100 & 100 & 100 & 0.46 \\ 100 & 100 & 100 & 100 & 100 & 0.63 \\ 100 & 100 & 100 & 100 & 100 & 0.38 \\ 100 & 100 & 100 & 100 & 100 & 0.36 \end{pmatrix}.$$

$T^{(0)}$ is normalized using (8) and (9), from which the DMs' weights are derived: $\lambda(T^{(0)}) = (0.1972, 0.2009, 0.2135, 0.1949, 0.1935)^T$. Using (3), the collective APR $P^{(c,0)}$ is

$$P^{(c,0)} = \begin{pmatrix} 0.5 & 0.3683 & 0.5878 & 0.5535 \\ 0.6317 & 0.5 & 0.5907 & 0.6150 \\ 0.4122 & 0.4093 & 0.5 & 0.5432 \\ 0.4465 & 0.3850 & 0.4568 & 0.5 \end{pmatrix}.$$

Based on the trust risk measurement rules, the third party monitors DMs' performance, the details are as follows:

1) From (17), the DMs' competence values, $\psi(P^{(1,0)}) = \psi(P^{(2,0)}) = \psi(P^{(5,0)}) = 0$ and $\psi(P^{(3,0)}) = \psi(P^{(4,0)}) = 2$, indicate that the logic and ability of DMs e_3 and e_4 are insufficient.
2) According to (2), DMs' consistency values are: $\mathrm{GCI}(P^{(1,0)}) = 0.0030$, $\mathrm{GCI}(P^{(2,0)}) = 0.4434$, $\mathrm{GCI}(P^{(3,0)}) = 1.5651$, $\mathrm{GCI}(P^{(4,0)}) = 1.4581$, and $\mathrm{GCI}(P^{(5,0)}) = 0.0363$. The values of $P^{(2,0)}$, $P^{(3,0)}$, and $P^{(4,0)}$ are greater than the corresponding threshold value $\overline{\mathrm{GCI}}$ (Table I), which means that DMs e_2, e_3 and e_4 do not satisfy the consistency property.
3) Using (20), $\epsilon^{(0)} = 0.1983$. From (18) and (19), the average fuzziness values $\overline{H}$ for DMs are: $\overline{H}(P^{(1,0)}) = 0.9420$, $\overline{H}(P^{(2,0)}) = 0.8315$, $\overline{H}(P^{(3,0)}) = 0.8849$, $\overline{H}(P^{(4,0)}) = 0.8306$, and $\overline{H}(P^{(5,0)}) = 0.8306$. Hence, except for DM e_1, all other DMs have an acceptable level of integrity at this round.
4) As for the DMs' fairness, it is obtained: $V^{(c,0)} = (0.4966, 0.5568, 0.4680, 0.4324)$, $V^{(1,0)} = (0.56, 0.66, 0.36, 0.56)$, $V^{(2,0)} = (0.24, 0.58, 0.47, 0.33)$, $V^{(3,0)} = (0.49, 0.28, 0.68, 0.48)$, $V^{(4,0)} = (0.78, 0.57, 0.49, 0.27)$, and $V^{(5,0)} = (0.42, 0.72, 0.32, 0.52)$. Equation (21) results in $s^{(3,0)} = s^{(4,0)} = 1$, which implies that DMs e_3 and e_4 lack fairness and are at risk of misleading others.
5) By (22), the receptivity of DMs is $r^{(1,0)} = 0.2187$, $r^{(2,0)} = 0.2625$, $r^{(3,0)} = 0.3062$, $r^{(4,0)} = 0.2729$, and $r^{(5,0)} = 0.2396$. It can be seen that all DMs' receptivity is recognized.

Then, using (28), $\mathrm{OEM}^{(0)}$ is constructed

$$\mathrm{OEM}^{(0)} = \begin{pmatrix} 100 & 100 & 85 & 100 & 100 \\ 100 & 85 & 100 & 100 & 100 \\ 85 & 85 & 100 & 85 & 100 \\ 85 & 85 & 100 & 85 & 100 \\ 100 & 100 & 100 & 100 & 100 \end{pmatrix}.$$

The weights of DMs' credibility are $\lambda(\mathrm{OEM}^{(0)}) = (0.2041, 0.2037, 0.1909, 0.1909, 0.2103)^T$. By (26), $\mathrm{TRI}^{(0)} = 0.8333 > \overline{\mathrm{TRI}}$. Thus, the group has a greater trust risk than accepted one, which prompts the third party to take effective measures to manage trust risk problems.

By (24) and (25), DM e_5 is identified as the DM with the highest trust risk level $\phi(e_5) = 4$, which lacks adequate trust. Consequently, the attributes evaluation of e_5 in $\mathrm{OEM}^{(0)}$ are increased using (30), and then the weight of e_5 is rewarded. Furthermore, MTAM $T^{(1)}$ and $\mathrm{OEM}^{(1)}$ are updated to

$$T^{(1)} = \begin{pmatrix} 100 & 100 & 85 & 100 & 100 & 0.41 \\ 100 & 85 & 100 & 100 & 100 & 0.46 \\ 85 & 85 & 100 & 85 & 100 & 0.63 \\ 85 & 85 & 100 & 85 & 100 & 0.38 \\ 100 & 100 & 100 & 100 & 100 & 0.36 \end{pmatrix}$$

$$\mathrm{OEM}^{(1)} = \begin{pmatrix} 100 & 100 & 85 & 100 & 100 \\ 100 & 85 & 100 & 100 & 100 \\ 85 & 85 & 100 & 85 & 100 \\ 85 & 85 & 100 & 85 & 100 \\ 115 & 115 & 115 & 115 & 115 \end{pmatrix}.$$

By (10), it is $\lambda(\mathrm{T}^{(1)}) = (0.2006, 0.2040, 0.2060, 0.1874, 0.2020)^T$ and $\lambda(\mathrm{OEM}^{(1)}) = (0.1979, 0.1975, 0.1851, 0.1851, 0.2344)^T$. At this round, the APRs of all DMs remain unchanged, and the collective APR is

$$P^{(c,1)} = \begin{pmatrix} 0.5 & 0.3604 & 0.5848 & 0.5478 \\ 0.6396 & 0.5 & 0.6052 & 0.6199 \\ 0.4152 & 0.3948 & 0.5 & 0.5314 \\ 0.4522 & 0.3801 & 0.4686 & 0.5 \end{pmatrix}.$$

As per (26), $\mathrm{TRI}^{(1)} = 0.6667 > \overline{\mathrm{TRI}}$, which again means that the group still has trust risk. By (25), DM e_3 has the maximum trust risk level $\phi(e_3) = 3$, and has the risk of blind trust. Using (27), the adjusted $P^{(3,2)}$ is obtained with the help of the APR of the highly reliable DM e_5

$$P^{(3,2)} = \begin{pmatrix} 0.5 & 0.25 & 0.6 & 0.55 \\ 0.75 & 0.5 & 0.5 & 0.5 \\ 0.4 & 0.5 & 0.5 & 0.5 \\ 0.45 & 0.5 & 0.5 & 0.5 \end{pmatrix}.$$

The updated MTAM $T^{(2)}$ based on $\mathrm{OEM}^{(1)}$ is

$$T^{(2)} = \begin{pmatrix} 100 & 100 & 85 & 100 & 100 & 0.41 \\ 100 & 85 & 100 & 100 & 100 & 0.46 \\ 85 & 85 & 100 & 85 & 100 & 0.63 \\ 85 & 85 & 100 & 85 & 100 & 0.38 \\ 115 & 115 & 115 & 115 & 115 & 0.36 \end{pmatrix}.$$

As per (10), $\lambda(T^{(2)}) = (0.1954, 0.1988, 0.2011, 0.1825, 0.2222)^T$. By (3), the collective APR $P^{(c,2)}$ is

$$P^{(c,2)} = \begin{pmatrix} 0.5 & 0.3503 & 0.5848 & 0.5177 \\ 0.6497 & 0.5 & 0.6856 & 0.6601 \\ 0.4152 & 0.3144 & 0.5 & 0.4911 \\ 0.4823 & 0.3399 & 0.5089 & 0.5 \end{pmatrix}.$$

The third party continues to oversee DMs' performance. During this iteration, only APR of DM e_3 is changed, so her/his performance also alters. Here, we only display the changed values: 1) by (17), the competence of DM e_3 is $\psi(P^{(3,2)}) = 2$; 2) the consistency degree of DM e_3 is $\mathrm{GCI}(P^{(3,2)}) = 0.3327$ by (2); 3) $\epsilon^{(2)} = 0.1683$ by (20). The value of average fuzziness $\overline{H}$ for DM e_3 is $\overline{H}(P^{(3,2)}) = 0.9590$ using (18) and (19); 4) the DMs' fairness: $V^{(c,2)} = (0.4843, 0.6088, 0.4249, 0.4404)$ and

$V^{(3,2)} = (0.455,\ 0.5,\ 0.5,\ 0.5)$; and 5) the receptivity of DMs are $r^{(1,2)} = 0.1812$, $r^{(2,2)} = 0.2375$, $r^{(3,2)} = 0.1812$, $r^{(4,2)} = 0.2521$, and $r^{(5,2)} = 0.1979$ by (22).

Using (29), the updated $\mathrm{OEM}^{(2)}$ is

$$\mathrm{OEM}^{(2)} = \begin{pmatrix} 100 & 100 & 70 & 100 & 100 \\ 100 & 70 & 100 & 100 & 100 \\ 70 & 85 & 85 & 85 & 100 \\ 70 & 70 & 100 & 70 & 100 \\ 115 & 115 & 115 & 115 & 115 \end{pmatrix}.$$

Hence, $\lambda(\mathrm{OEM}^{(2)}) = (0.2006,\ 0.1997,\ 0.1806,\ 0.1738,\ 0.2454)^T$. As per (26), $\mathrm{TRI}^{(2)} = 0.3333 < \overline{\mathrm{TRI}}$. In other words, the group is now with admissible trust risk.

Thus, the updated MTAM $T^{(2)'}$ by merging $\mathrm{OEM}^{(2)}$ is

$$T^{(2)'} = \begin{pmatrix} 100 & 100 & 70 & 100 & 100 & 0.41 \\ 100 & 70 & 100 & 100 & 100 & 0.46 \\ 70 & 85 & 85 & 85 & 100 & 0.63 \\ 70 & 70 & 100 & 70 & 100 & 0.38 \\ 115 & 115 & 115 & 115 & 115 & 0.36 \end{pmatrix}.$$

Using (10), the reasonable DMs' weights are obtained: $\lambda(T^{(2)'}) = (0.1977, 0.2007, 0.1974, 0.1731, 0.2312)^T$. By (3), the credible collective APR $P^{(c,2)'}$ is

$$P^{(c,2)'} = \begin{pmatrix} 0.5 & 0.3460 & 0.5814 & 0.5168 \\ 0.6540 & 0.5 & 0.6892 & 0.6608 \\ 0.4186 & 0.3108 & 0.5 & 0.4862 \\ 0.4832 & 0.3392 & 0.5138 & 0.5 \end{pmatrix}.$$

According to (14) and (15), the conflict level of the individual DM and the group are calculated: $\theta^{(1,2)} = 0.0912$, $\theta^{(2,2)} = 0.1671$, $\theta^{(3,2)} = 0.0853$, $\theta^{(4,2)} = 0.1886$, $\theta^{(5,2)} = 0.1196$, and $\theta^{(c,2)} = 0.1287 < \delta$. Thus, the predefined conflict level is achieved.

Finally, the exploitation process with (4) results in $QGDD(x_1) = 0.4808$, $QGDD(x_2) = 0.6107$, $QGDD(x_3) = 0.4230$, and $QGDD(x_4) = 0.4426$, which translates in the final consensus collective ranking of alternatives: $x_2 \succ x_1 \succ x_4 \succ x_3$.

The proposed model is a new decision model that considers both trust risk management and conflict elimination. In order to emphasize the feasibility and validity of the developed model, we compare it with the calculation results of the traditional CEP, as shown in Table IX. Obviously, the proposed model has great advantages both in the control of trust risks and the promotion of consensus. The group's TRI is reduced from 0.8333 to 0.3333, which is more than 50%. Also, the number of the DMs with trust risks is significantly reduced, with a drop of 60%. The traditional CEP has no effect on the changes of these two values. Moreover, the proposed model reduced the level of conflict without increasing the number of iterations. That is to say, the proposed method can effectively promote consensus and increase the success rate. On the other hand, we find that the ranking results of these two methods are different, which is natural and logical. In the traditional CEP, the DMs' weights are often related to trust relationship and are static. If the DM with low credibility is given a higher weight, it may mislead the final decision result. However, in the proposed decision process, we consider DMs' credibility, reconcile the difference between credibility and external trust, so that the highly credible DM e_5 can be given enough attention in group, rather than aggregating information based on external trust relationship. Meanwhile, the information modification for the blindly trusted DM e_3 is inspired by the more credible DM e_5, which further ensures the rationality of the decision result. Therefore, the proposed framework allows making more reasonable and credible decision.

TABLE IX
COMPARISON RESULTS BETWEEN OUR PROPOSAL AND TRADITIONAL CEP

Method	*TRI*	TRMD	r	r'	DR	t	$\theta^{(c)}$	Ranking result
Our proposal	0.3333	50%	5	2	60%	2	0.1287	$x_2 \succ x_1 \succ x_4 \succ x_3$
Traditional CEP	0.8333	0	5	5	0	2	0.1669	$x_2 \succ x_1 \succ x_3 \succ x_4$

VI. CONCLUSION

This article reported the development of a novel trust risk analysis-based CEP in SNGDM. In this framework, a third-party organization is introduced to monitor the performance of DMs in CEP and to provide evaluation information on DMs. Subsequently, a trust risk measurement method and dynamic management mechanism are designed to detect and reduce the trust risk level of group. Finally, the DMs' weights integrated into the CEP are dynamically derived from an MTAM. Simulation experiments supported the effectiveness of our proposal in trust risk management.

The developed approach can offer decision support to help DMs address the following trust risk problems in SNGDM: blind trust and lack of logical trust. This can prevent DMs from being misled by their close relationship with someone or someone's status in the SN, and obtain more reasonable and reliable decision results in SNGDN.

With the development of information technology, large-scale GDM has become a hot issue. In the large-scale GDM environment, the trust risk problems will become more complicated. Thus, in future research, it will be worthy and interesting to devise an effective mechanism for managing the trust risks in large-scale GDM [26].

REFERENCES

[1] Y. C. Dong *et al.*, "Consensus reaching in social network group decision making: research paradigms and challenges," *Knowl. Based Syst.*, vol. 162, pp. 3–13, Dec. 2018.

[2] Y. C. Dong, H. J. Zhang, and E. Herrera-Viedma, "Integrating experts' weights generated dynamically into the consensus reaching process and its applications in managing non-cooperative behaviors," *Decis. Support Syst.*, vol. 84, pp. 1–15, Apr. 2016.

[3] J. Wu, R. Xiong, and F. Chiclana, "Uninorm trust propagation and aggregation methods for group decision making in social network with four tuple information," *Knowl. Based Syst.*, vol. 96, no. 2, pp. 29–39, Mar. 2016.

[4] J. Wu, F. Chiclana, H. Fujita, and E. Herrera-Viedma, "A visual interaction consensus model for social network group decision making with trust propagation," *Knowl. Based Syst.*, vol. 122, pp. 39–50, Apr. 2017.

[5] R. Ureña, G. Kou, Y. C. Dong, F. Chiclana, and E. Herrera-Viedma, "A review on trust propagation and opinion dynamics in social networks and group decision making frameworks," *Inf. Sci.*, vol. 478, pp. 461–475, Apr. 2019.

[6] J. Wu, S. Wang, F. Chiclana, and E. Herrera-Viedma, "Two-fold personalized feedback mechanism for social network consensus by uninorm interval trust propagation," *IEEE Trans. Cybern.*, early access, May 18, 2021, doi: 10.1109/TCYB.2021.3076420.

[7] X. Liu, Y. Xu, R. Montes, and F. Herrera, "Social network group decision making: Managing self-confidence-based consensus model with the dynamic importance degree of experts and trust-based feedback mechanism," *Inf. Sci.*, vol. 505, pp. 215–232, Dec. 2019.

[8] P. Pettit, "The cunning of trust," *Philos. Publ. Affairs*, vol. 24, no. 3, pp. 202–225, 1995.

[9] T. K. Das and B.-S. Teng, "The risk-based view of trust: A conceptual framework," *J. Bus. Psychol.*, vol. 19, no. 1, pp. 85–116, 2004.

[10] J. Xu and C. Fung, "A risk-defined trust transitivity model for group decisions in social networks," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, 2019, pp. 415–420.

[11] G. Kambourakis, "Anonymity and closely related terms in the cyberspace: An analysis by example," *J. Inf. Secur. Appl.*, vol. 19, no. 1, pp. 2–17, 2014.

[12] S. Singh and D. Chand, "Trust evaluation in cloud based on friends and third party's recommendations," in *Proc. Recent Adv. Eng. Comput. Sci. (RAECS)*, 2014, pp. 1–6.

[13] Z. G. Wu, H. Y. Xu, and G. Y. Ke, "The strategy of third-party mediation based on the option prioritization in the graph model," *J. Syst. Sci. Syst. Eng.*, vol. 28, no. 4, pp. 399–414, 2019.

[14] J. K. Butler, "Toward understanding and measuring conditions of trust: evolution of a conditions of trust inventory," *J. Manag.*, vol. 17, no. 3, pp. 643–663, 1991.

[15] S. A. Orlovsky, "Decision-making with a fuzzy preference relation," *Fuzzy Sets Syst.*, vol. 1, no. 3, pp. 155–167, 1978.

[16] T. Tanino, "Fuzzy preference orderings in group decision making," *Fuzzy Sets Syst.*, vol. 12, no. 2, pp. 117–131, 1984.

[17] M. M. Xia, Z. S. Xu, and J. Chen, "Algorithms for improving consistency or consensus of reciprocal [0, 1]-valued preference relations," *Fuzzy Sets Syst.*, vol. 216, pp. 108–133, Apr. 2013.

[18] T. L. Saaty, *The Analytic Hierarchy Process*. New York, NY, USA: McGraw-Hill, 1980.

[19] Y. J. Xu, M. Q. Li, F. J. Cabrerizo, F. Chiclana, and E. Herrera-Viedma, "Algorithms to detect and rectify multiplicative and ordinal inconsistencies of fuzzy preference relations," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 6, pp. 3498–3511, Jun. 2021.

[20] J. Aguarón and J. M. A. Moreno-Jiménez, "The geometric consistency index: Approximated thresholds," *Eur. J. Oper. Res.*, vol. 147, no. 1, pp. 137–145, 2003.

[21] Y. J. Xu, R. Patnayakuni, and H. M. Wang, "The ordinal consistency of a fuzzy preference relation," *Inf. Sci.*, vol. 224, pp. 152–164, Mar. 2013.

[22] R. R. Yager, "On ordered weighted averaging aggregation operators in multicriteria decision making," *IEEE Trans. Syst., Man, Cybern.*, vol. 18, no. 1, pp. 183–190, Jan./Feb. 1988.

[23] F. Chiclana, F. Herrera, and E. Herrera-Viedma, "Integrating three representation models in fuzzy multipurpose decision making based on fuzzy preference relations," *Fuzzy Sets Syst.*, vol. 97, no. 1, pp. 33–48, 1998.

[24] L. G. Pérez, F. Mata, and F. Chiclana, "Social network decision making with linguistic trustworthiness-based induced OWA operators," *Int. J. Intell. Syst.*, vol. 29, no. 12, pp. 1117–1137, 2014.

[25] A. Khalid and I. Beg, "Role of honesty and confined interpersonal influence in modelling predilections," *Soft Comput.*, vol. 24, pp. 1497–1509, Jan. 2020.

[26] M. Tang, H. C. Liao, E. Herrera-Viedma, C. L. P. Chen, and W. Pedrycz, "A dynamic adaptive subgroup-to-subgroup compatibility-based conflict detection and resolution model for multicriteria large-scale group decision making," *IEEE Trans. Cybern.*, vol. 51, no. 10, pp. 4784–4795, Oct. 2021.

Mengqi Li is currently pursuing the Ph.D. degree from the Business School, Hohai University, Nanjing, China, and the Andalusian Research Institute on Data Science and Computational Intelligence, University of Granada, Granada, Spain.

Her current research interests include decision making analysis, consensus reaching process, hesitant fuzzy set, and large-scale decision making.

Yejun Xu received the M.S. and Ph.D. degrees in management science and engineering from Southeast University, Nanjing, China, in 2005 and 2009, respectively.

He is currently a Professor with the College of Management and Economics, Tianjin University, Tianjin, China. He has contributed over 140 journal articles to professional journals, such as IEEE TRANSACTIONS ON FUZZY SYSTEMS, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, *Fuzzy Sets and Systems*, and *Knowledge-Based Systems*. His current research interests include multiple criteria decision making and computing with words.

Xia Liu received the Ph.D. degree in management science and engineering from Hohai University, Nanjing, China, in 2020.

She is currently an Associate Professor with the School of Management Science and Engineering, Nanjing University of Information Science and Technology, Nanjing. Her current research interests include large-scale group decision making, decision support systems, hesitant fuzzy set, and consensus reaching process.

Francisco Chiclana received the B.Sc. and Ph.D. degrees in mathematics from the University of Granada, Granada, Spain, in 1989 and 2000, respectively.

He is a Professor of Computational Intelligence and Decision Making with the School of Computer Science and Informatics, Faculty of Computing, Engineering and Media, De Montfort University, Leicester, U.K. From 2015 to 2018, he was Honorary Professor with the Department of Mathematics, University of Leicester, Leicester. He is currently a Visiting Scholar with the Department of Computer Science and Artificial Intelligence, University of Granada.

Prof. Chiclana is an associate editor and a guest editor for several ISI-indexed journals. Clarivate Analytics has currently classed him as a Highly Cited Researcher in Computer Sciences. He has organized and chaired special sessions/workshops in many major international conferences in research areas as fuzzy preference modeling, decision support systems, consensus, recommender systems, social networks, rationality/consistency, and aggregation.

Francisco Herrera (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in mathematics from the University of Granada, Granada, Spain, in 1988 and 1991, respectively.

He is currently a Professor with the Department of Computer Science and Artificial Intelligence and the Director of DaSCI Institute (Andalusian Research Institute on Data Science and Computational Intelligence), University of Granada. He has been the Supervisor of 42 Ph.D. students. He has published more than 400 journal papers, receiving more than 60 000 citations (Scholar Google, H-index 122). He has coauthored the books *Genetic Fuzzy Systems* (World Scientific, 2001), *Data Preprocessing in Data Mining* (Springer, 2015), *The 2-tuple Linguistic Model. Computing With Words in Decision Making* (Springer, 2015), and *Multilabel Classification. Problem Analysis, Metrics and Techniques* (Springer, 2016). His current research interests include among others, computational intelligence (including fuzzy modeling, computing with words, evolutionary algorithms, and deep learning), information fusion and decision making, and data science (including data preprocessing, prediction, and big data).

Prof. Herrera received the following honors and awards, including the ECCAI Fellow 2009, the IFSA Fellow 2013, the 2010 Spanish National Award on Computer Science ARITMEL to the "Spanish Engineer on Computer Science," the International Cajastur "Mamdani" Prize for Soft Computing (Fourth Edition, 2010), the *IEEE Transactions on Fuzzy Systems* Outstanding 2008 and 2012 Paper Award (bestowed in 2011 and 2015 respectively), the 2011 Lotfi A. Zadeh Prize Best paper Award (IFSA Association), the 2013 AEPIA Award to a scientific career in Artificial Intelligence, the 2014 XV Andalucía Research Prize Maimónides, the 2017 Security Forum I+D+I Prize, and the 2017 Andalucía Medal (by the regional government of Andalucía). He has been selected as a Highly Cited Researcher http://highlycited.com/ (in the fields of Computer Science and Engineering, respectively, since 2014, Clarivate Analytics). He acts as an editorial member of a dozen of journals. He currently acts as an Editor-in-Chief of the international journals *Information Fusion* (Elsevier) and *Progress in Artificial Intelligence* (Springer).