

A review on trust propagation and opinion dynamics in social networks and group decision making frameworks

Raquel Ureña, Gang Kou, Yucheng Dong, Francisco Chiclana, Enrique Herrera-Viedma

▶ **To cite this version:**

Raquel Ureña, Gang Kou, Yucheng Dong, Francisco Chiclana, Enrique Herrera-Viedma. A review on trust propagation and opinion dynamics in social networks and group decision making frameworks. Information Sciences, 2018, 478, pp.461 - 475. 10.1016/j.ins.2018.11.037 . inserm-03026204

HAL Id: inserm-03026204

https://inserm.hal.science/inserm-03026204

Submitted on 26 Nov 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Information Sciences 478 (2019) 461–475

Contents lists available at ScienceDirect

Information Sciences

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

A review on trust propagation and opinion dynamics in social networks and group decision making frameworks

Raquel Ureña[a,*], Gang Kou[b], Yucheng Dong[c], Francisco Chiclana[a,d,*], Enrique Herrera-Viedma[d,e,*]

[a] Institute of Artificial Intelligence (IAI), School of Computer Science and Informatics, De Montfort University, Leicester, UK
[b] School of Business Administration, Southwestern University of Finance and Economics, Chengdu, China
[c] Business School, Sichuan University, Chengdu, China
[d] Department of Computer Science and Artificial Intelligence, University of Granada, Granada, Spain
[e] Peoples' Friendship University of Russia (RUDN University), Moscow, Russian Federation

ARTICLE INFO

Article history:
Received 19 August 2018
Revised 12 November 2018
Accepted 17 November 2018
Available online 19 November 2018

Keywords:
Trust
Reputation
Influence
Social networks
Decision making
Opinion dynamics

ABSTRACT

On-line platforms foster the communication capabilities of the Internet to develop large-scale influence networks in which the quality of the interactions can be evaluated based on trust and reputation. So far, this technology is well known for building trust and harnessing cooperation in on-line marketplaces, such as Amazon (www.amazon.com) and eBay (www.ebay.es). However, these mechanisms are poised to have a broader impact on a wide range of scenarios, from large scale decision making procedures, such as the ones implied in e-democracy, to trust based recommendations on e-health context or influence and performance assessment in e-marketing and e-learning systems. This contribution surveys the progress in understanding the new possibilities and challenges that trust and reputation systems pose. To do so, it discusses trust, reputation and influence which are important measures in networked based communication mechanisms to support the worthiness of information, products, services opinions and recommendations. The existent mechanisms to estimate and propagate trust and reputation, in distributed networked scenarios, and how these measures can be integrated in decision making to reach consensus among the agents are analysed. Furthermore, it also provides an overview of the relevant work in opinion dynamics and influence assessment, as part of social networks. Finally, it identifies challenges and research opportunities on how the so called trust based network can be leveraged as an influence measure to foster decision making processes and recommendation mechanisms in complex social networks scenarios with uncertain knowledge, like the mentioned in e-health and e-marketing frameworks.

© 2019 The Authors. Published by Elsevier Inc.
This is an open access article under the CC BY license.
(http://creativecommons.org/licenses/by/4.0/)

* Corresponding authors.
E-mail addresses: raquel.urena@dmu.ac.uk (R. Ureña), kougang@swufe.edu.cn (G. Kou), ycdong@scu.edu.cn (Y. Dong), chiclana@dmu.ac.uk, inv.chiclana@ugr.es (F. Chiclana), viedma@decsai.ugr.es (E. Herrera-Viedma).

https://doi.org/10.1016/j.ins.2018.11.037
0020-0255/© 2019 The Authors. Published by Elsevier Inc. This is an open access article under the CC BY license.
(http://creativecommons.org/licenses/by/4.0/)

1. Introduction

Virtual interactions between people and services without any previous real world relationship have experienced an exponential increase with the availability of interactive on line sites, including the so called social networks. These interconnected platforms present very diverse functionalities; from the well known social networks Facebook (www.facebook.com), Instagram (www.instagram.com) or Twitter (www.twitter.com), where people share pictures and thoughts with their friends and followers, to e-commerce platform like Amazon or E-bay; crowd-sourcing platforms to share knowledge and expertise, such as Wikipedia (www.wikipedia.com), Slashdot (www.slashdot.com), or Quora (www.quora.com), and on-line facilities sharing networks such as UBER (www.uber.com) and Blablacar (www.blablacar.com) for cars or Airbnb (www.airbnb.com/) for accommodation. In spite of the diversity of the available on-line communities, all of them share the common characteristic of having a vast amount of users interacting between each other under a virtual identity. These emerging social media channels permit users to build various explicit or implicit social relationships, to leverage the network as a worldwide showcase to disseminate and share products, services, information, opinions and recommendations.

In these digital media scenarios, the evaluation of the credibility of the information constitutes a more challenging problem than in conventional media, because of its inherent anonymous, open nature that is characterised by a lack of strong governance structures [23]. In fact, this anonymity offers a favourable environment for malicious users to spread wrong information, virus, or even files in the case of Peer to Peer networks (P2P) [26]. Therefore, it is necessary to use mechanisms that allow to choose the peers from whom interact as well as effectively identify and isolate the malicious ones.

The ideal solution would be to develop a web of reputation and trust, either at a local level (individual websites for example) or across the whole web, that would enable users to express and propagate trust on others to the entire network to allow other users to assess the quality of the information or service provided even without a prior interaction with the agent in question. The ultimate goal, here, is to estimate, for each agent, a reputation level or score. In this sense, reputation can be understood as a predictor of future behaviour based on previous interactions, that is, any agent will be considered as highly regarded if it has consistently performed satisfactorily in the past assuming that the service can be trusted to perform as expected in the future as well. Therefore, reputation and trust based management will ultimately lead to minimise poor and dishonest agents as well as to encourage the reliable and trustworthy behaviours [17,22,30], which, in its turn, makes reputation to be one key mechanism for the social governance on the Internet [49].

When it comes to estimate reputation and propagate trust, we can recognise two main differences between traditional and on-line environments: (i) traditional indicators that allow to estimate trust and reputation, observed on the physical world, are missing in on-line environments, and so electronic substitutes are required; (ii) in the physical world, communicating and sharing information related to trust and reputation is relatively difficult, since this knowledge is constrained to local communities. On the contrary, in the case of IT systems, the Internet can be leveraged to design efficient ways to calculate and propagate this information in a world-wide scale [30].

Some examples of these on-line reputation networks are included in e-commerce platforms such as Amazon and E-bay or even in accommodation booking platforms like Airbnb where both hosts and guests are rated with the aim to provide a global reputation score publicly available to all users. With this regards, it has been observe that a reliable reputation system increases users trust on the Web [9]. In fact, for the case of e-auctions systems several studies confirm that reputation mechanisms benefit both sellers and buyers [27]. More concretely, for the case of e-Bay it has been concluded that part of the e-Bay's commercial success can be attributed to its reputation mechanism, eBay's Feedback Forum, that allows as well to rate negatively dishonest behaviour [19].

On the other hand, trust has been considered as well an important factor to influence decision making and consensus reaching between multiple users in group decision making (GDM) scenarios [5,33,38,39,41]. These procedures facilitate agents to negotiate in order to arrive to mutually acceptable agreements [3,32,46], and so trust here can be used to spread experts opinions and to provide recommendations [44,45,47]. A recent survey on social network based consensus approaches [11] points out that trust based GDM approaches are still in an early stage and they lack the necessary tools to calculate dynamically inter agents trust and influence.

The aim of this article is to survey the main mechanisms to generate and propagate trust and reputation in social networks and to point out several open questions concerning the integration of trust and reputation based measures and opinion dynamics procedures in the context of decision making approaches. To do so, this contribution is organised as follows: Section 2 analyses the main characteristics of on-line social communities. Section 3 introduces the concepts of trust and reputation, and the differences between them. The main existing procedures to estimate reputation and to propagate trust are also explained in this section. Section 4 focuses on the trust based GDM approaches, while the main approaches to carry out opinion spreading in social networks are revised in Section 5. The main challenges and research opportunities on how the analysed trust and reputation based systems, as an influence measure to foster decision making processes and recommendation mechanisms in complex social networks scenarios with uncertain knowledge, are pointed out in Section 6. Finally, conclusions are presented Section 7.

2. Social networks

A social network can be considered as a set of people (or even groups of people) that participate and interact sharing different kinds of information with the purpose of friendship, marketing or business exchange. Social network modelling refers to the analysis of the different structures in the network to understand the underlying pattern that may either facilitate or impede the knowledge creation in this type of interconnected communities [21].

2.1. Characteristics of real world social networks

A multi person social network has some specific characteristics, when compared with a random graph of nodes, that have to be considered in order to properly understand the opinion dynamics, trust propagation and influence. In the following, some of the most important ones are pointed out:

A small-world network

The two main structural properties that define this type of network are the higher clustering coefficient and average path length that scales the logarithm of the number of nodes. The clustering coefficient is also known as the transitivity, that is, a friend of a friend is likely to be my friend and the average path length is the minimum number of nodes to traverse to move from A to B [21].

Scale free network

This implies that few nodes present an elevated number of connections (degree) whereas the majority of them present very few connections. These type of networks have no specific scales for the degrees.

In a social network, it is key to identify which agents or individuals cause the highest influence in the network, and which are the nodes that receive this impact. The *eigenvector centrality* proposed by Bonacich and Lloyd [2] has been extensively adopted as a measure of the relative importance of an individual in a social influence network. In this way, centrality scores are given to all the nodes in the network based on the premise that "the centrality or status of an individual is a function of the status of those who choose him", for example, being chosen by someone powerful makes one more powerful to the eyes of the others. Thus, a node having a high eigenvector centrality means that it is connected to other nodes with high eigenvector centrality as well. This measures can be mathematically formalised as follows:

Definition 1 (Centrality [2])**.** Given an adjacency Matrix $A = (a_{ij})$, with element a_{ij} represents the degree of influence of node i towards node j and let $\mathbf{v} = (v_1, \ldots, v_i, \ldots, v_n)$ the unknown vector of centrality scores for each node, then

$$v_i = v_1 a_{1i} + v_2 a_{2i} + \cdots + v_n a_{ni},$$

Which can be expressed as the following eigenvector equation

$$A^T \mathbf{v} = \mathbf{v}.$$

Notice that this eigenvector based centrality assessment may not be applicable to asymmetric networks. For these cases, a generalisation of this measure, that allows every individual some status that does not depend only on his or her connection to others, denominated α-centrality has been proposed in [2]. This assumes for example that the popularity of each student in a class depends not only on her internal connections with her fellow students within the class but also on her independent external evaluation by other such as her teachers. Therefore, given the vector e that represents this external (exogenous) sources of status or information the above expression can be extended as follows:

$$v = \alpha A^T v + e.$$

3. Trust and reputation systems

Trust and reputation management encompasses several disciplines such us data collection and storage, modelling, communication, evaluation and reputation safeguards [30]. Therefore, various research initiatives have been carried out in different sectors ranging from psychology, sociology and politics to economics, computer science and marketing. From the perspective of computer science, examples of existing applications that make use of reputation and or trust approaches include peer-to-peer (P2P) networks, e-commerce, e-marketing, multi-agent systems, web search engines and GDM scenarios.

Manifestation of trust are almost obvious in our daily routine; nevertheless finding an exact definition is challenging since trust can be represented in many different forms leading to an ambiguous concept. In cite [22], the following *definition of trust* is provided: "trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible." The authors claim that this relative vague definition encompasses the following aspects: "(i) *dependence* on the party that is trusted; (ii) *reliability of the trusted entity*; (iii) *utility* a positive utility will result from a positive outcome, and negative utility will result from a negative outcome; (iv) *risk attitude* that implies the trusting party is willing to accept a possible risk."

On the other hand, according to the Concise Oxford dictionary, "*reputation* is what is generally said or believed about a person's or thing's character or standing." This definition is aligned with the one given by social networks researchers

that states that "reputation is a quantity measure derived from the underlying social network which is globally visible to all members of the network" [13]. Therefore reputation can be understood as the perception that an agent creates through past actions about its intentions and norms in a global level. Reputation can be assessed in relation with one individual or with a whole group. For example group reputation can be obtained as the average of all its individual members' reputation values. Indeed it has been observed that the fact that an individual belongs to a given group has an impact in his/her reputation depending on the give group's reputation.

Notice that the concept of reputation is closely linked to that of trustworthiness, since dependence and reliability, which are key implications in the definition of trust, can be assessed through a persons reputation, for example, based on the evaluations given by the other members in the system. Therefore trust can be established through the use of reputation. That is, one may trust someone who has a good reputation. However, the difference between trust and reputation resides in that trust systems take into consideration as input general and subjective measures of trust (reliability) in a pairwise basis, whereas reputation considers the information about objective events like specific transactions [22].

Trust manifestations from traditional systems include subjective terms of friendship, long term based knowledge or even intuition that are not available in on-line system. Thus, electronic measures are required to computerise these abstracts concepts. Conversely, in real physical worlds, trust and reputation systems are confined to small local communities and so the use of IT technologies in a proper way will allow the effective development of worldwide systems to exchange and collect trust based knowledge. Some challenges arise in this regard: (i) finding effective ways to model and recognise trust and reputation in the on-line world, i.e. to identify the available cues and develop mechanisms to fuse them; (ii) mechanisms to collect and propagate these measures in a scalable, secure, and robust way. According to Kamvar et al. [26], there are six main characteristics that any on-line trust and reputation system should address:

1. *Self policing.* The system should rely on the information given by the users of the network and not on some central authority, therefore ratings given by the user about current interactions should be collected and distributed.
2. *Durability in time of the entities.* After an interaction it is normally assumed that a posterior interation will take place in the future.
3. *Anonymity.* The reputation and trust should be link with an ID.
4. *No profit to newcomers.* Reputation is calculated by constant good behaviour, no advantages for new members.
5. *Minimal overhead.* The computation of the values of trust and reputation should not constitute a charge in terms of computation to the whole system.
6. *Robust to malicious collectives.* Users trying to abuse of the trust system should be immediately recognised and blocked in the system.

In the following the main characteristics of the trust and reputation systems are analysed. To do so, in Section 3.1 the main reputation network architectures are presented. In Section 3.2, the procedures to compute reputation are outlined. In Section 3.3, the principal approaches to carry out trust propagation between peers are studied. Finally in Section 3.4, an overview of various methods that use both reputation and trust are presented.

3.1. Reputation network architectures

In a reputation system, once a transaction between two agents is completed the agents are required to rate the quality of the transaction (service). The architecture of the these systems determines the way in which the ratings and reputation scores are collected, stored and shared between the members of the system. There exist two main types of reputation network architectures (see Fig. 1): centralised and distributed.

In a centralised reputation system (Fig. 1(a)) a central authority collects all the ratings and constantly updates each agent's reputation score as a function of the rating the agent received. This type of system requires (i) a centralised communication protocol in charge of keeping the central authority updated from all the ratings; and (ii) a reputation calculation method for the central authority to estimate and update the reputation of each agent. In contrast, in a distributed reputation system (Fig. 1(b)) each agent individually collects and combines the ratings from the other agents. That is, an agent A, who wants to transact with another target agent B, has to demand for ratings to the other community members who have directly interacted with agent B. Consequently, given the distributed nature of the information, obtaining the ratings from all interactions with a given agent may be too expensive (time consuming) and so, only a subset of the interactions, usually from the relying agents' network are considered to calculate the reputation score. This type of system requires (i) a distributed communication protocol to allow agents to get information from others agent they are considering to transact with; and (ii) a reputation computation method to estimate and update the reputation given the values of other agents (neighbours). A well known example of distributed architecture are P2P networks in which each agent acts as both client and server. It is noted that these networks may introduce a security threat since they could be used to propagate malicious software or to bypass firewalls. Therefore the role of reputation in this particular case is crucial to determine which nodes in the network are most reliable and which ones should be avoided.

3.2. Reputation calculation

In the following the most popular mechanisms to compute reputation are outlined.

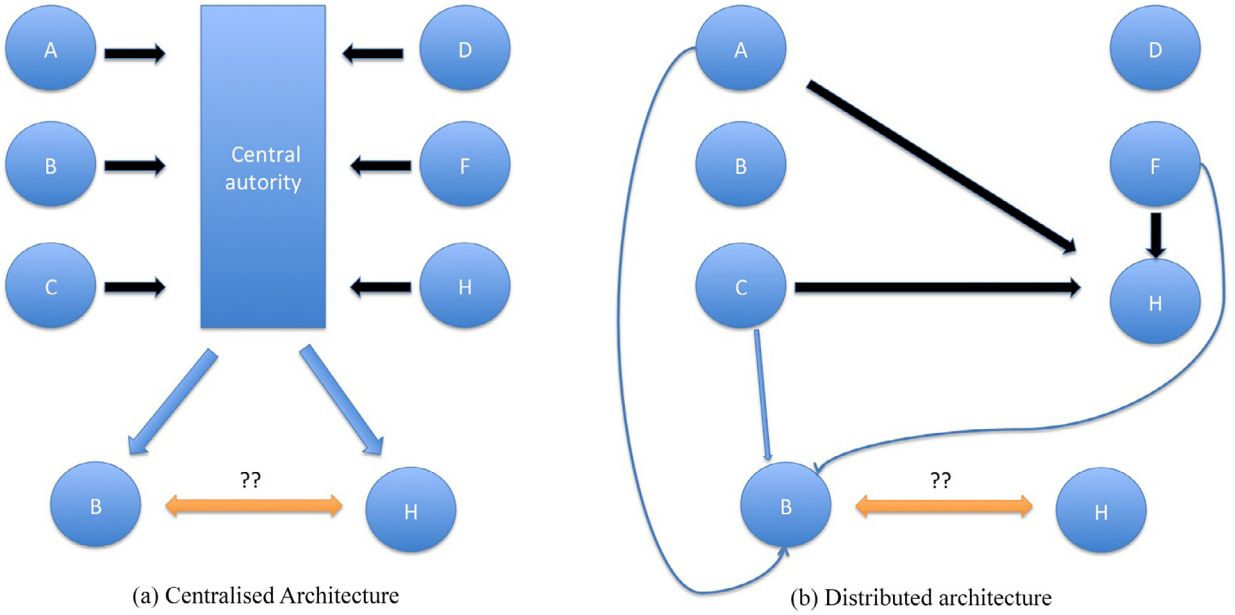


Fig. 1. Architecture for reputation systems.

Counting

This simple technique consists in the summation of the positive ratings minus the summation of negative ones. This is the technique proposed by e-Bay [34]. An alternative related approach is Amazon's one based a weighted average of the ratings taking into consideration factors such as rater trustworthiness, distance between ratings and current scores [36].

Probabilistic models

These models use as input previous binary ratings, positive or negative, to estimate the probability of a future transaction to be positive or negative [18,22]. The β-probability distribution is a family of continuous probability distributions that has been used in Bayesian analysis to describe initial knowledge concerning probability of success. Its expression relies on the gamma function γ in the following way:

$$\beta(p|\alpha,\beta) = \frac{\gamma(\alpha+\beta)}{\gamma(\alpha)\gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1},$$

where $0 \le p \le 1$, $\alpha,\ \beta > 0$, with expectation value being $E(p|\alpha,\beta) = \frac{\alpha}{\alpha+\beta}$. In the reputation framework of interest in this paper, α and β represent the amount of positive and negative ratings, respectively.

Fuzzy models

They use of fuzzy numbers or linguistic ratings modelled as fuzzy sets with membership functions describing the extent up to which an agent can be trustworthy or not. Examples of this approach are the Regret System proposed by Sabater and Sierra [35] and trust based GDM methodologies [45–47] that will be discussed in more detail in the next section.

3.3. Trust propagation approaches

In a social network, where the agents have express their trust on other agents, there might not be direct trust relationship between all pair of agents of the network. The goal of a trust propagation system is to estimate unknown trust values between pair of agents using the known and available trust values (see Fig. 2). Thus, given a network of n agents, who may have expressed some of their level of trust (and/or distrust), and $T = (t_{ij})$ being the matrix of trust values where $t_{ij}(\in [0, 1])$ represents the agent i trust value on agent j, there may be the case that some of the elements of matrix T are unknown. The estimation of the trust value between any two agents with no previous interaction between them, has been proposed to be carried out by some authors using models that rely on some kind of transitive property of trust via an iterative transitivity based aggregation along the different paths in the network that connect indirectly both agents until the estimated trust scores become stable for all agents. These models are based on the premise that a user is more likely to trust the statements/recommendations/advices coming from a trusted user. In this way, trust may propagate (with appropriate mitigation) through the network [15]. These models are known as Flow Reputation Systems [17,22]. In what follows a review of the two most representative mechanisms is presented.

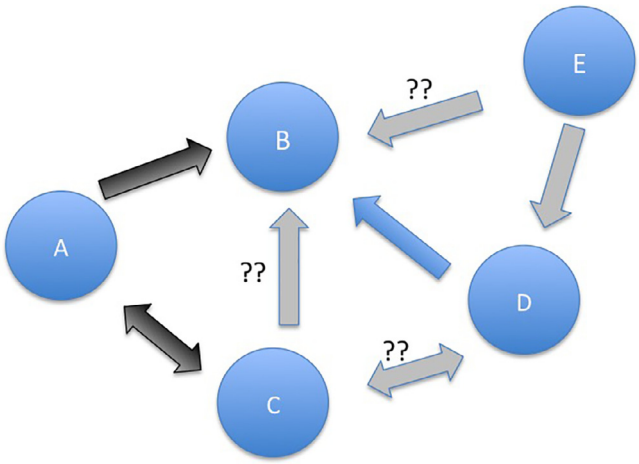


Fig. 2. Trust propagation problem.

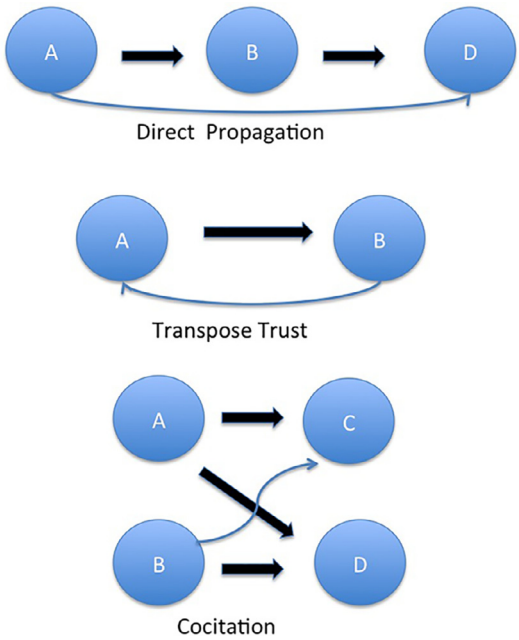


Fig. 3. Guha et al.'s trust propagation approach.

Guha's et al. model [15]

This approach estimates the trust missing values carrying out atomic propagation of the trust in four different ways (the first three are depicted in Fig. 3):

- *Direct propagation:* Given the value of $t_{ij} = 1$ meaning that i trusts j, and $t_{jk} = 1$ indicating j trusts k, then it concludes that i trusts k by means of an atomic direct propagation where the trust propagates directly along an edge.
- *Transpose trust:* Given that i trusts j then j might present some level of trust towards i.
- *Co-citation:* In this case the agent i_1 trusts j_1 and j_2, and agent i_2 trusts j_2. The co-citation propagation assumes that agent i_2 may trust agent j_1 as well.
- *Trust coupling:* Given that i trusts j then this trust propagates to k when j and k trust agents in common.

The above four types of trust propagation can combined into a single matrix $C^k_{B,w}$ based on a belief matrix, B, and a weight vector, $W = (w_1, w_2, w_3, w_4)$, as follows: $C^k_{B,w} = w_1 B + w_2 B^T B + w_3 B^T + w_4 B B^T$.

With this approach, distrust can also be propagated. With respect to rust propagation, it is obvious that if i trusts j, and j trusts k, then i might have a "positive" predisposition towards k based on this knowledge. However, with respect to distrust,

this transitivity of trust might not hold, which stems from the complexity of trust and distrust representing peoples multi-dimensional utility functions. To overcome this issue the authors propose two corresponding algebraic notions of distrust propagation: (1) the first one, known as multiplicative distrust propagation, is based on the premise that the enemy of your enemy may be your friend; and (2) the second one, denominated additive distrust propagation, is based on the notion that if your enemy do not trust someone, you should not trust this person either.

In order to propagate both trust and distrust, Guha et al. propose three different schema that varies in the way the belief matrix, B, and the matrix of propagation after k steps, $P(k)$, are generated by taking into account or not the distrust values:

- *Trust only.* The distrust value is completely ignored in this case so trust scores are propagated.

$$B = T; P(k) = C^k_{B,w}.$$

- *One-step distrust.* In this case it is assumed the additive distrust propagation, that is, if a user does not trust someone all the judgments of this person are discarded, and so distrust propagates only one step whereas trust propagates recursively.

$$B = T; P(k) = C^k_{B,w} \times (T - D),$$

where D ($d_{ij} \in [0, 1]$) is the distrust matrix.

- *Propagate distrust.* In this case it is assumed that both trust and distrust are propagated together, and so they are processed as the two ends of a continuum.

$$B = T - D; P(k) = C^k_{B,w}.$$

Kamvar's et al. approach [26]

This approach is also based on the notion of transitivity but without distrust propagation. In addition, in contrast to the pairwise approach used in Guha's et al. model [15], for each node this approach calculates a global measure of trust with the following twofold aim: (i) to isolate malicious agents from the network and encouraging agents to interact with reputable ones; and (ii) to motivate the agents to interact by rewarding the reputable ones.

This approach works as follows: each time agent i interacts with agent j, the transaction may be rated as positive ($tr_{i,j} = 1$) or negative ($tr_{i,j} = -1$); then, a local trust value s_{ij} is defined as the sum of the ratings of the individual transactions that agent i had with agent j: $s_{ij} = \sum tr_{ij}$; equivalently, each agent i can store the number of satisfactory $sat(i, j)$ and unsatisfactory, $unsat(i, j)$, transactions with agent j, with $s_{ij} = sat(i, j) - unsat(i, j)$. In distributed systems, as it is the case here, the challenge is to aggregate the local trust values without using a central storage capacity. To do so, Kamvar et al. demonstrate that transitivity of trust leads to a system where global trust values correspond to the left principal eigenvector of a matrix of normalised local trust values.

On the other hand, in order to avoid malicious users who might assign arbitrary high values to other malicious peers and arbitrary low values to the good ones, the scores values are normalised when aggregating local trust values

$$c_{ij} = \frac{max(s_{ij}, 0)}{\sum_j max(s_{ij}, 0)}.$$

Following this normalisation, the aggregation is carried out by asking the peer i's acquaintances about their opinions on other peers, which are weighted by the trust peer i places on them. In this way, the trust value that peer i gives to peer k, based on the questioning of the peer i's friends, is computed as follows

$$t_{ik} = \sum_j c_{ij} c_{jk}.$$

3.4. Trust and reputation distributed approaches

In this section we present some examples of systems that combines both trust and reputation.

- *RateWeb* [30] is a decentralised and unstructured approach that calculates trust between web services. In order to select the appropriate service, the trusting entity queries the community for a list of suitable service providers. This set of eligible services providers is returned with a list of past entities that have used the service. In this case, each agent stores a personal perception of the services it has interacted with, and the reputation of each service based on this feedback is calculated as follows:

$$Rep_i = \frac{\sum_{j=1}^{L} t_{ij} \lambda_f Cr_j}{\sum_{j=1} Cr_j},$$

where L denotes the set of trusting agents that have interacted with the service i; t_{ij} represents the pairwise trust value that agent j has on i; $Cr_j \in [0, 1]$ is the credibility of each trusting entity, as viewed by the inquiring entity, and $\lambda_f \in [0, 1]$ is a trust with time decay factor.

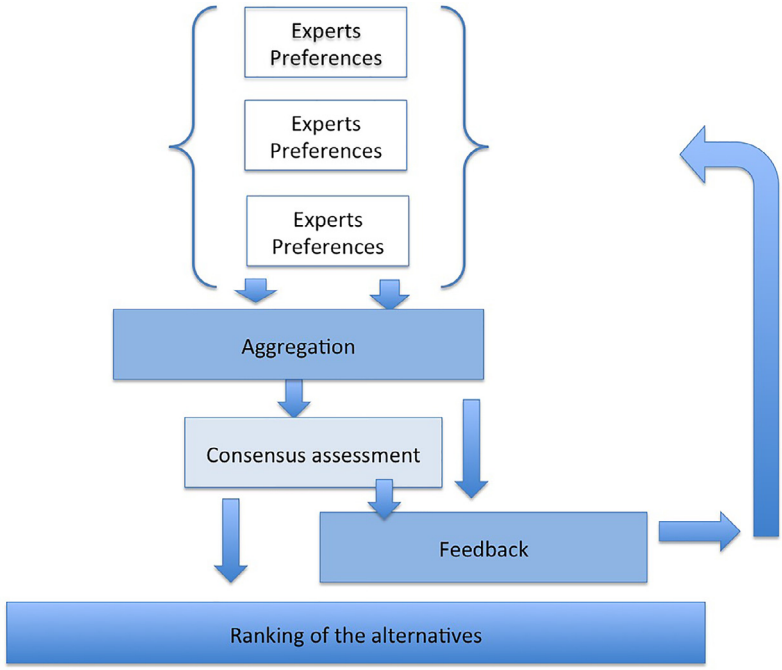


Fig. 4. GDM scenarios architecture.

- *R2Trust* [37] is an example of a fully distributed system in which the reputation of an agent in the network is calculated by aggregating the direct interaction of this entity as well as obtaining recommendations. The value of the recommendation is weighted in the aggregation using local pairwise trust values, which are probabilistic ratings between zero and one calculated as a function of the past interaction. These trust values are calculated using the social relationships, with the particularity that it includes the inherent risk in these relationships. These values are then aggregated and accumulated to give an entity a reputation value using a credibility score weighting mechanism to filter out untrustworthy second-hand opinions. The main advantage of this approach is that, thanks to the risk assessment, is able to react quickly when there is an irregular variation on the behaviour of a given peer. In this case the reputation is calculated as follows:

$$DT_{ij} = \frac{\sum_{k=1}^{n} \lambda_k e_{ij}^{tk}}{\sum_{k=1}^{n} \lambda_k},$$

where $\lambda_k = p(nk)$ is the decay factor of time period k; $0 \le \lambda_k \le \lambda_{k+1} \le 1,\ 1 \le k \le n$; and e_{ij}^{tk} denotes a local trust value of entity i on entity j over the time period t_k.
- *GRAft* [17] is a distributed reputation system, whose main peculiarity is that it uses both explicit reputation information (like scores and ratings) and implicit information (such as the in-degree and out-degree in a social network). This reputation information is gathered and stored in the form of XML based profiles. This system does not process this information, instead, it proposes logical policies to generate trust based on the users' profile.
- Another decentralised graph-based reputation model has been proposed in [49], which makes use of social context, including the behavioural activities and social relationship of the opinion contributors, to fully build the trust relationships even in scenarios with scarce first-hand information. In order to attenuate the subjectivity of opinions and the dynamics of behaviours, a set of critical trust factors are pointed out. For example, a deception filtering approach able to recognise malicious agents is included to discard bad-mouthing opinions and personalised direct distrust propagation. This system develops a multi-graph based social network in which the users are characterised and interconnected by means of the following criteria: (i) the context of each performed activity; (ii) the values associated with each activity and relationship; (iii) all the performed activities; and (iv) all the social relationships of the users.

4. Trust based social network decision making approaches

Group decision making is an example scenario in which multiple agents interact to obtain a solution. Nowadays there is an emergent trend that considers this process in the context of a large scale social network with multiple agents negotiating their opinions by means of feedback to reach a solution of consensus [4,40,50]. Generally GDM processes are composed of four main stages as depicted in Fig. 4

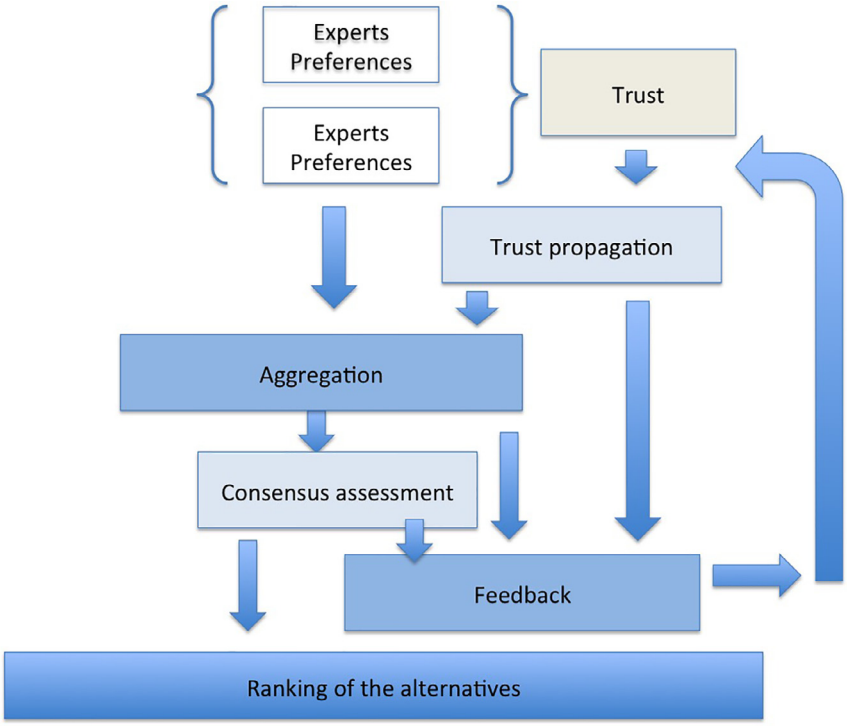


Fig. 5. GDM scenarios architecture with trust.

Agents preference elicitation

At this first stage the experts provide their opinions. In many approaches the use of fuzzy sets is considered in order to handle uncertainty in the experts' opinions. As explained later, if trust is included in the procedure, then a mechanism to propagate trust between the members taking part in the process is developed. Moreover, there could be cases where some experts may provide incomplete information [41], and so a process to estimate the missing information may be included taking into account the trust between the experts.

Opinion aggregation

At this stage the opinions coming from the different agents are fused. Here trust may play a key role since the opinion of the agents may be weighed according to their associated trust values.

Consensus calculation

At this stage, the level of similarity between the agents' opinions is computed in order to assess whether an acceptable level of group agreement has been reached.

Feedback

At this stage personalised feedback are produced and provided to all or some members of the network to consider in a negotiation process with the aim to bring the experts' opinion closer and, consequently, to facilitate the reaching of group consensus.

Recently trust and reputation have been consider as key elements in group decision negotiation processes. Fig. 5 shows an scheme that summarises the stages where trust may play a role in these scenarios. In the following an analysis of the main approaches that use trust in group decision making scenarios is presented from three different perspectives: (i) trust propagation; (ii) trust based opinion fusion; and (iii) trust modelling.

4.1. Trust propagation in GDM

In [44] a social network based group decision making approach is presented in which the information about trust, and distrust are jointly propagated among the members of the network by means of a t-norm operator following the methodol-

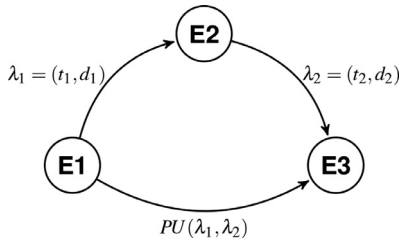


Fig. 6. Trust propagation network.

ogy presented in [42], where the *t*-norm and the *t*-conorm operators were used to propagate trust and distrust, respectively. Specifically, it is proposed a trust propagation mechanism based on the transitivity property of the *t*-norm operator that can be formally expressed as follows:

$$P((t_1, d_1), (t_2, d_2), \ldots, (t_n, d_n)) = (TN(t_1, t_2, \ldots, t_n), TN(t_1, t_2, \ldots, t_{n-1}, d_n)),$$

where TN represents a *t*-norm operator and $\delta = \{\lambda = (t, d) | t, d \in [0, 1]\}$ is the set of orthopairs of trust (t)/distrust (d) values, which are referred to as trust functions $\lambda = (t, d)$ (TFs).

Wu et al. pointed out in [47] that using two different operators to independently propagate information might not be optimal since trust and distrust are not independent. Moreover the authors remark that the t-norm tends to favour the minimum value in the aggregation whereas the *t*-conorm favours maximum values, and so, this predictable behaviour suppose a vulnerability in the system in case of malicious user. For this reason, in [47], unify the propagation of both trust and distrust with the implementation of an uninorm operator, which generalise both *t*-norms and *t*-conorm operator. In general, a *t*-norm operator behaves like a *t*-norm operator when all values are below the identity element; in the case of all the values being higher than the identity element it behaves like a *t*-conorm; otherwise it behaves like a symmetric mean operator.

Definition 2. Let U be a uninorm operator. A uninorm trust propagation operator PU is a mapping, PU: $\delta \times \delta \to \delta$, that associates two TFs, $\lambda_1 = (t_1, d_1)$ and $\lambda_2 = (t_2, d_2)$, with the following trust function value output: $PU(\lambda_1, \lambda_2) = (U(t_1, t_2), U(t_1, d_2))$.

The type of uninorm operator used in [47] is the well known and like representable cross ratio uninorm which, according to [7], is the most convenient for handling appropriately inconsistent information. When estimating trust between two distant nodes in a social network if more than one indirect path between them exists, then it is proposed to use the shortest one, that is, the one with minimum number of intermediate nodes. For example, given the scenario represented in Fig. 6, to estimate the trust and distrust values between E1 and E3 the following premises are followed:

- Trust propagation: in a complete trust/distrust scenario, it is expected that when expert E1 fully trusts E2 and expert E2 fully trusts E3 then E1 will fully trust E3.
- Distrust propagation: expert E1 will fully distrust E3 when expert E2 fully distrusts E3 and expert E1 fully trusts E2.

4.2. Trust based opinion fusion

In decision making scenarios it is usually necessary to aggregate the individual opinions before arriving at a collective solution. In the recent literature on fuzzy decision making, Yager's Order Weighted Averaging (OWA) operator [48] has been widely used. This operator allocates different importance degree to the aggregated elements based on their ordering with respect to certain criteria of interest, a characteristic that has been shown to be very effective against malicious behaviour [10].

In [47], the properties of the cross ratio uninorm sum of TFs and the uninorm scalar multiplication of a TF by a natural number are used to formally define the uninorm trust weighted average (UTWA) operator that uses trust as a measure to calculate the weights and the ordering in the aggregation OWA aggregation. Recently in [46], the authors have proposed an extension of this approach that takes advantage of all the possible paths to estimate trust and distrust and fuse all of them using and OWA operator taking into account the risk attitude of the members of the network. Moreover, this approach uses trust to provide recommendations to the experts to estimate their incomplete preferences. On the other hand, in [45] the set of experts are represented by means of a directed graph in which the edges represent the trust among the given experts. In this case, in order to assess the importance of each expert in the aggregation, the authors propose to calculate the in-degree centrality of each node in the network, and this value, when normalised, is employed to calculate the weights and to induce the ordering of the values in an IOWA aggregation.

4.3. Trust modeling

In most of the contributions analysed so far, trust has been modelled by means of a crisp or binary relation, that is only two possible states are assumed: 'trusting' and 'not trusting'. However, in real life situations, trust can be interpreted

Table 1
Summary of the trust and reputation approaches analysed.

Reference	Year	Architecture	Trust/distrust	Trust Computation	Local/global	Application
[36]	2000	Centralised	Trust	Counting	Global	e-commerce
[35]	2001	Centralised	Trust/reputation	Fuzzy	Global	General
[34]	2002	Centralised	Trust	Counting	Global	e-commerce
[26]	2003	Distributed	Trust	Counting	Global	P2P
[15]	2004	Distributed	Trust and distrust	Counting	Pairwise	General
[18]	2009	Distributed	Trust	Probabilistic	Local	Security
[30]	2009	Distributed	Reputation	Multiple sources	Global	Web services
[42]	2009	–	Trust/distrust	t-norm/t-conorm	Pairwise	Rec. systems
[37]	2011	Distributed	Reputation	Past interaction	Pairwise	General
[17]	2015	Distributed	Reputation	Explicit/implicit	Global	General
[49]	2015	Distributed	Reputation	Social context	Global	e-commerce
[17]	2015	Distributed	Reputation	Explicit/implicit	Global	General
[44]	2015	–	Trust/distrust	t-norm	Pairwise	GDM
[47]	2016	–	Trust/distrust	Uninorm,	Pairwise	GDM
[29]	2017	–	Interval trust	–	Pairwise	GDM
[46]	2018	–	Trust/distrust	Uninorm	Pairwise	GDM
[45]	2018	–	Linguistic trust	–	Pairwise	GDM

as a “gradual concept” with people trusting someone ‘high’, ‘middle’ and/or ‘low’ [42]. In [45], the concept of distributed linguistic trust is defined to establish the trust relationship between a group users, while in [29] the concept of trust is proposed to be modelled as an interval-valued trust function and definitions are provided for interval-valued trust score, interval-valued knowledge degree, and ranking order relation for interval-valued trust functions, within the aim to achieve more flexibility in the expression of opinions to include trust, distrust, hesitancy and conflict. This last approach propagates trust between experts following the premise that decision makers may trust opinions coming from trusted experts in their vicinity. Therefore, the concept of trust degree is defined based on the distance between two experts without taking into account other aspects such as the reputation of the experts or the interactions between them [31], which is subsequently used in a recommendation mechanism to increase the consensus.

Table 1presents in chronological order the main contributions, and their main characteristics, that have been analysed in Sections 3 and 4.

5. Opinion dynamics

Opinion dynamics can be regarded, on the context of social networks, as the way in which the network is created and evolves provoking individuals’ attitudes, opinions and behaviours toward particular objects to change taking into consideration the displayed attitudes, opinions, and behaviours of other individuals toward the same object [8,12,40]. Opinion formation and evolution is closely linked with trust between the members of the network because the opinion of the individuals are related with the opinion of individual who trust each other, and as well the trust that an individual may give to another one is conditioned by the opinion of trust of other trusted individuals. Thus, a social influence networks can be defined as a social structure composed of members dealing with a common issue [14,20,24,25]. These networks can be mathematically formulated as follows:

Definition 3. *Social influence network:* A directed influence network is an ordered triple, $G_S =< N, T, W >$, comprising a set of nodes N connected by a set of ties T with a set of influence weights W attached to T, where w_{ij} represents the influence to agent j by agent i and $W = [w_{ij}],\ w_{ij} \in [0, 1] \forall i, j,\ \sum_j w_{ij} = 1\ \forall i$.

In the literature we can find two main mathematical models for opinion dynamics, the DeGroot model [8] and its generalisation proposed by Friedkin and Johnsen [14].

DeGroot model [8]

This model considers the opinion evolution of the individuals as a weighted average of their opinions at a previous time state, using the following recursively mathematical formulation

$$y(t+1) = Wy(t),\ \ t = 0, 1, 2, \ldots$$

where $y(t)$ is a real-valued vector representing the individuals’ opinions at time t.

Friedkin and Johnsen (FJ) model [14]

This model, which generalises the DeGroot model, considers as well how individual opinions evolve with respect to their previous state opinions, and it is supported by work reported in [20] that empirically proves the assumption that individuals

update their opinions via a convex combinations of their own and others' displayed opinions, based on weights that are automatically generated by individuals in their responses to the displayed opinions of other individuals. The mathematical formulation of the FJ Model being

$$y(t+1) = (I_n - \delta)Wy(t) + \delta y(0), t = 0, 1, 2, \ldots$$

According to the FJ model, when opinion formation reaches equilibrium (consensus or a deadlock), the final opinions can be predicted by mean of combining the following three elements:

1. $y(t)$ is a column vector representing the opinions of the members of the network at time state t, with $y(0)$ representing their initial opinions.
2. $\delta = diag(\delta_{11}, \delta_{22}, \ldots, \delta_{nn})$ is the susceptibility of actors to interpersonal influences and I_n $n \times n$ identity matrix. DeGroot model [8] is a special case of FJ model when $\delta_{ii} = 0, 1 \leq i \leq n$.
3. $W = \left(w_{ij}\right)_{m\times m}$ is a row represents actors relative importance (row elements sums equal 1) on others preferences including themselves, i.e. w_{ij} represents the direct importance that actor i gives to the opinion held by actor j.

Particular cases of the FJ model are the so called bounded confidence models. According to these models, each agent uniquely interacts with the agents who hold similar opinions. This similarity of opinions can be seen as a confidence level between agents. Therefore in these models, the similarity between agents as well as their initial opinions determine the opinion of a neighbourhood in which the expert is likely to interact at every instant. The two main bounded confidence-based models are the Hegselmann–Krause (HK) model [16] and the Deffuant–Weisbuch (DW) model [43], which consist of three main steps:

Step1: each agent's confidence set (neighbourhood) is determined: given a confidence level $\epsilon > 0$; $\forall i$: determine $j \in \{1, \ldots, n\}$ such that $|y_i(t) - y_j(t)| \leq \epsilon$;
Step 2: each agent's degrees of influence with respect to a given one is computed ($W = \left(w_{ij}\right)_{m\times m}$); and
Step 3: the opinion for each agent is updated.

- The HK model mathematical formulation for the opinion update is:

$$y_i(t+1) = \frac{\sum_{j:|y_i(t)-y_j(t)|\leq\epsilon} w_{ij}y_j(t)}{\sum_{j:|y_i(t)-y_j(t)|\leq\epsilon} w_{ij}}$$

- The HK model mathematical formulation for the opinion update is:

$$\begin{cases} y_i(t+1) = y_i(t) + \lambda[y_j(t) - y_i(t)] \\ y_j(t+1) = y_j(t) + \lambda[y_i(t) - y_j(t)] \end{cases}$$

  where λ is a convergence parameter.

The main difference between these two models is that the DW model adopts an asynchronous opinion updating process, whereas the HK model adopts a synchronous updating process.

6. Discussion and open research challenges

Motivated by the analysis and observations carried out in this research survey, the following research challenges are highlighted:

Identifying sources of trust and reputation in the digital world susceptible of being explicitly and/or implicitly estimated

The majority of commercial systems available rely on their users providing an explicit feedback regarding their degree of satisfaction with the interaction with other users [17]. This approach has the advantage of allowing to obtain direct feedback in a simple way. Nevertheless, direct rating suffers from several drawbacks, such as the low motivation of users to rate, unfair and biased ratings and the ballot box stuffing (more ratings than the legitimate expected number of ratings) [17,22]. In on-line interconnected systems, though, there is much more information available that can be used to extract implicit information about trust and reputation between users. For example two individuals that interact regularly are likely to trust each other. In this regard, mechanisms of behaviour scoring could be designed and developed to assess, in an automatic way, the reputation of agents. Thus, the following two challenges deserve future research efforts to address them: (1) recognising patterns of behaviour related to the reputation level. (2) Merging global behaviour evaluation with pairwise interaction between users to assess peer to peer related trust.

Similarity measures could be useful to assess trust between users. For example, in opinion dynamics models, it has been proved that users tend to consider and trusting more other users with similar opinions to them [16,24,25,40,45]. The challenge resides in this case in the characterisation of similarity measures that captures the relevant features for two users to be considered as similar and so they can trust each other.

Propagation of trust

In order to estimate the trust value between two agents that have not previously interacted, the flow model has been proposed, which relies in the transitivity property of trust and the existence of at least one indirect path in the local network connecting both agents. An important challenge here is the assessment of the degree of coherence of the estimated trust, i.e. according to the known values of trust of an agent, will it be pertinent to use the transitivity property to estimate the missing trust values? This measure of coherence may be used a priori to evaluate whether the transitivity property would be adequate to be used to propagate trust.

Dealing with malicious users

In reputation systems, a common malicious behaviour is associated with unfair ratings. In other words, when demanding feedback from users about how an interaction was, some of the users may act in a malicious way with a given purpose, for example, to manipulate the score towards the benefit of certain entities. Another common malicious behaviour is the so called 'ballot box stuffing', that consists in getting more ratings than the legitimate number of expected ratings. The main approaches to detect and minimise these fraudulent behaviours are:

- Endogenous discounting. These mechanisms takes advantages of the statistical properties of the ratings to allocate less importance or even exclude the ratings that presumably may be unfair.
- Exogenous discounting. These approaches are based on the premise that the raters with low reputation usually provide unfair valuations, which can be weighted down accordingly.
- Providing ratings just after the transaction has been completed. This is good practice to avoid ballot box stuffing.

The challenge in this case resides in the developing of mechanisms to flag malicious behaviour users. In this sense, techniques based on game theory may play a key role [6] together with the use of an OWA-based operator [48], which has been proved to be better than a weighted average operator to mitigate malicious behaviour in the information aggregation processes [10].

Reputation and trust in GDM systems

As mentioned before, GDM scenarios can be considered as a specific case of social network in which the users interact to reach a decision where it is desired to reach consensus. It is usual for a GDM process to include a negotiation process in which the agents are asked to provide recommendations to other agents. In this scenario the following three research challenges are identified:

- *Modelling trust in GDM frameworks.* In dealing with trust, the existing decision making approaches assume that pairwise trust values are given, and if there are unknown trust values (not given by experts) these are estimated using a transitivity based trust propagation procedure. In order to avoid malicious behaviour, and as well to liberate the user from rating their peers, other mechanisms of trust calculation are necessary which could be based on measures of centrality [13], to give an example. An initial effort, in this sense, has been carried out in [40,45] where the trust has been modelled based on the concept of proximity of experts' opinions [31].
- *Interpersonal influence, trust and reputation aggregation for recommendations.* Within this context it is key to leverage the power of the trust based network in decision making processes using the trust between agents as a measure of influence, not only in e-commerce scenarios but in e-democracy, e-learning and e-health platforms as well [1,28]. With the objective of deploying this idea, we identify two main open questions:
  (i) How to aggregate both influence and trust in a decision process. In this sense, there are some initial efforts where trust based aggregation of the experts' opinions are carried out using a trust induced IOWA operator [44,45]. A further endeavour in this context is to extend the opinion dynamics and propagation approaches by including trust assessment and analyse how the propagation of both influence and trust could be done.
  (ii) Integrating trust in complex scenarios where users are heterogeneous, and both reputation and trust may be in conflict, as it might happen in an e-health network to provide recommendations where we can have users with different profiles, and relevance levels such us doctors and patients.
- *Reputation based expert selection.* In a trust network of peers there may be a large corpus of experts where not all of them will be part in the decision and therefore it is necessary to choose whom will be involved, for which reputation could be used, and avoid disclosing sensible information to experts whose reputation is low, as applied in P2P networks, in what it is call the search phase.

7. Conclusion

Nowadays on-line services and communities play a prominent role in people's life, from communication and buying purposes to advice seeking for decision making, or recommendations. Nevertheless, the inherent anonymity and open architecture of these systems make difficult for the users to build trust relations among their peers in the network. It is, in

this context, where trust and reputation mechanisms play an increasingly important role in order to facilitate users interactions. Therefore, it is not surprising the rich literature growing around these mechanisms for on-line communities and in commercial applications. In this contribution we have analysed these approaches and presented a survey of the main trust propagation and reputation schemes. Moreover, opinion dynamics models, which allows to identify both leaders and followers in a social network environment, are currently being investigated with the aim of identifying new opportunities together with both trust and influence propagation. From this study, we have found that the main areas of application of trust and reputation systems are e-commerce, P2P networks and it is increasingly used in GDM models. However, these mechanisms are poised to have a larger impact on a wide range of scenarios, ranging from large scale decision making procedures, such as the ones implied in e-democracy, trust based recommendations on e-health scenarios or influence and performance assessment in e-marketing and e-learning systems. In this regard, we have pointed out various research challenges that deserves further attention: (i) identifying new implicit and explicit sources of trust and reputation; (ii) trust and influence propagation in decision making approaches; (iii) trust based missing information estimation; (iv) dealing with malicious users via game theory methodologies; and (v) exploiting trust to carry out experts selection. To conclude, it is important to remark that there is not a single solution that can be applied in all contexts. Therefore the challenge when developing a new system is to tailor it to the specific constraints imposed by each application, and the type of information that can be used for the ratings, striking a balance between reliability, security and users acceptability.

Acknowledgements

The authors acknowledge the financial support from the EU project H2020-MSCA-IF-2016-DeciTrustNET-746398, FEDER funds provided in the National Spanish project TIN2016-75850-P, and the support of the RUDN University Program 5-100 (Russian Federation).

References

[1] L. Alboaie, S.C. Buraga, Trust and reputation in e-health systems, in: Proceedings of the International Conference on Advancements of Medicine and Health Care through Technology, Springer, Berlin, Heidelberg, 2009, pp. 43–48.
[2] P. Bonacich, P. Lloyd, Eigenvector-like measures of centrality for asymmetric relations, Soc. Netw. 23 (2001) 191–201.
[3] F. Cabrerizo, F. Chiclana, R. Al-Hmouz, A. Morfeq, A. Balamash, E. Herrera-Viedma, Fuzzy decision making and consensus: challenges, J. Intell. Fuzzy Syst. 29 (2015) 1109–1118.
[4] F.J. Cabrerizo, R. Ureña, W. Pedrycz, E. Herrera-Viedma, Building consensus in group decision making with an allocation of information granularity, Fuzzy Sets Syst. 255 (2014) 115–127.
[5] N. Capuano, F. Chiclana, H. Fujita, E. Herrera-Viedma, V. Loia, Fuzzy group decision making with incomplete information guided by social influence, IEEE Trans. Fuzzy Syst. 26 (2018) 1704–1718.
[6] M. Chica, R. Chiong, M. Kirley, H. Ishibuchi, A networked n-player trust game and its evolutionary dynamics, IEEE Trans. Evol. Comput. (2018), doi:10.1109/TEVC.2017.2769081.
[7] F. Chiclana, E. Herrera-Viedma, S. Alonso, F. Herrera, Cardinal consistency of reciprocal preference relations: a characterization of multiplicative transitivity, IEEE Trans. Fuzzy Syst. 17 (2009) 14–23.
[8] M. DeGroot, Reaching a consensus, J. Am. Stat. Assoc. 69 (1974) 118–121.
[9] C. Dellarocas, The digitization of word of mouth: promise and challenges of online feedback mechanisms, Manag. Sci. 49 (2003) 1407–1424.
[10] Y. Dong, Y. Liu, H. Liang, F. Chiclana, E. Herrera-Viedma, Strategic weight manipulation in multiple attribute decision making, Omega (Westport) 75 (2018) 154–164.
[11] Y. Dong, Q. Zha, H. Zhang, G. Kou, H. Fujita, F. Chiclana, E. Herrera-Viedma, Consensus reaching in social network group decision making: research paradigms and challenges, Knowl. Based Syst. (2018), doi:10.1016/j.knosys.2018.06.036.
[12] Y. Dong, M. Zhan, G. Kou, Z. Ding, H. Liang, A survey on the fusion process in opinion dynamics, Inf. Fusion 43 (2018) 57–65.
[13] L.C. Freeman, Centrality in social networks: conceptual clarification, Soc. Netw. 1 (1979) 215–239.
[14] N.E. Friedkin, E.C. Johnsen, Social Influence Network Theory: A Sociological Examination of Small Group Dynamics, Cambridge University Press, New York, 2014.
[15] R. Guha, R. Kumar, P. Raghavan, A. Tomkins, Propagation of trust and distrust, in: Proceedings of the Thirteenth International Conference on World Wide Web, 2004, pp. 403–412.
[16] R. Hegselmann, U. Krause, Opinion dynamics and bounded confidence, models, analysis and simulation, J. Artif. Soc. Soc. Simul. 5 (2002) 1–33.
[17] F. Hendrikx, K. Bubendorfer, R. Chard, Reputation systems: a survey and taxonomy, J. Parallel Distrib. Comput. 75 (2015) 184–197.
[18] K. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Comput. Surv. 42 (2009) 1:1–1:31.
[19] D. Houser, J. Wooders, Reputation in auctions: theory, and evidence from eBay, Econ. Manag. Strat. 15 (2005) 353–369.
[20] P. Jia, A. MirTabatabaei, N.E. Friedkin, F. Bullo, Opinion dynamics and the evolution of social power in influence networks, SIAM Rev. 57 (2015) 367–397.
[21] J. Scott, Social Network Analysis: A Handbook, SAGE Publications, New York, 2000.
[22] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2007) 618–644.
[23] G. Kambourakis, Anonymity and closely related terms in the cyberspace: an analysis by example, J. Inf. Secur. Appl. 19 (2014) 2–17.
[24] N.H. Kamis, F. Chiclana, J. Levesley, Geo-uninorm consistency control module for preference similarity network hierarchical clustering based consensus model, Knowl. Based. Syst. (2018), doi:10.1016/j.knosys.2018.05.039.
[25] N.H. Kamis, F. Chiclana, J. Levesley, Preference similarity network structural equivalence clustering based consensus group decision making model, Appl. Soft Comput. 67 (2018) 706–720.
[26] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina, The eigentrust algorithm for reputation management in P2P networks, in: Proceedings of the Twelfth International Conference on World Wide Web, ACM, 2003, pp. 640–651.
[27] C. Keser, Experimental games for the design of reputation management systems, IBM Syst. J. 42 (2003) 498–506.
[28] W. Liu, Y. Dong, F. Chiclana, F.J. Cabrerizo, E. Herrera-Viedma, Group decision-making based on heterogeneous preference relations with self-confidence, Fuzzy Optim. Decis. Mak. 16 (2017) 429–447.
[29] Y. Liu, C. Liang, F. Chiclana, J. Wu, A trust induced recommendation mechanism for reaching consensus in group decision making, Knowl. Based Syst. 119 (2017) 221–231.
[30] Z. Malik, A. Bouguettaya, RATEWeb: reputation assessment for trust establishment among web services, VLDB J. 18 (2009) 885–911.
[31] M.J. del Moral, F. Chiclana, J.M. Tapia, E. Herrera-Viedma, A comparative study on consensus measures in group decision making, Int. J. Intell. Syst. 33 (2018) 1624–1638.

[32] I.J. Pérez, F.J. Cabrerizo, E. Herrera-Viedma, A mobile decision support system for dynamic group decision-making problems, IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum. 40 (2010) 1244–1256.
[33] I. Pérez, F. Cabrerizo, S. Alonso, Y. Dong, F. Chiclana, E. Herrera-Viedma, On dynamic consensus processes in group decision making problems, Inf. Sci. (NY) 459 (2018) 20–35.
[34] P. Resnick, R. Zeckhauser, M.R. Baye, Trust among strangers in internet transactions: empirical analysis of eBays reputation system, in: The Economics of the Internet and E-commerce (Advances in Applied Microeconomics Volume 11), Emerald Group Publishing Limited, 2002, pp. 127–157.
[35] J. Sabater, C. Sierra, Social regret, a reputation model based on social relations, SIGecom Exch. 3 (1) (2002) 44–56.
[36] J. Schneider, G. Kortuem, J. Jager, S. Fickas, Z. Segall, Disseminating trust information in wearable communities, Pers. Ubiquitous Comput. 4 (2000) 245–248.
[37] C. Tian, B. Yang, R2Trust: a reputation and risk based trust management framework for large-scale, fully decentralized overlay networks, Fut. Gen. Comput. Syst. 27 (2011) 1135–1141.
[38] R. Ureña, F.J. Cabrerizo, J.A. Morente-Molinera, E. Herrera-Viedma, GDM-R: a new framework in R to support fuzzy group decision making processes, Inf. Sci. (NY) 357 (2016) 161–181.
[39] R. Ureña, F. Chiclana, H. Fujita, E. Herrera-Viedma, Confidence-consistency driven group decision making approach with incomplete reciprocal intuitionistic preference relations, Knowl. Based Syst. 89 (2015) 86–96.
[40] R. Ureña, F. Chiclana, G. Melançn, E. Herrera-Viedma, A social network based approach for consensus achievement in multiperson decision making, Inf. Fusion 47 (2019) 72–87.
[41] R. Ureña, F. Chiclana, J. Morente-Molinera, E. Herrera-Viedma, Managing incomplete preference relations in decision making: a review and future trends, Inf. Sci. (NY) 302 (2015) 14–32.
[42] P. Victor, C. Cornelis, M. De Cock, P. Pinheiro da Silva, Gradual trust and distrust in recommender systems, Fuzzy Sets Syst. 160 (2009) 1367–1382.
[43] G. Weisbuch, G. Deffuant, F. Amblard, J.P. Nadal, Meet, discuss, and segregate!, Complexity 7 (2002) 55–63.
[44] J. Wu, F. Chiclana, E. Herrera-Viedma, Trust based consensus model for social network in an incomplete linguistic information context, Appl. Soft. Comput. 35 (2015) 827–839.
[45] J. Wu, L. Dai, F. Chiclana, H. Fujita, E. Herrera-Viedma, A minimum adjustment cost feedback mechanism based consensus model for group decision making under social network with distributed linguistic trust, Inf. Fusion 41 (2018) 232–242.
[46] J. Wu, L. Dai, F. Chiclana, H. Fujita, E. Herrera-Viedma, A new consensus model for social network group decision making based on a minimum adjustment feedback mechanism and distributed linguistic trust, Inf. Fusion 41 (2018) 232–242.
[47] J. Wu, R. Xiong, F. Chiclana, Uninorm trust propagation and aggregation methods for group decision making in social network with four tuple information, Knowl. Based Syst. 96 (2016) 29–39.
[48] R.R. Yager, Quantifier guided aggregation using OWA operators, Int. J. Intell. Syst. 11 (1996) 49–73.
[49] S.R. Yan, X.L. Zheng, Y. Wang, W.W. Song, W.Y. Zhang, A graph-based comprehensive reputation model: exploiting the social context of opinions to enhance trust in social commerce, Inf. Sci. (NY) 318 (2015) 51–72.
[50] H. Zhang, Y. Dong, E. Herrera-Viedma, Consensus building for the heterogeneous large-scale GDM with the individual concerns and satisfactions, IEEE Trans. Fuzzy Syst. 26 (2018) 884–898.