Trust and Reputation Models for Multiagent Systems

JONES GRANATYR, Research Group of Computational Intelligence – University of Contestado - UnC
VANDERSON BOTELHO, PPGIa: Graduate Program on Informatics –
Pontifical Catholic University of Paraná – PUCPR
OTTO ROBERT LESSING, Research Group of Computational Intelligence –
University of Contestado - UnC
EDSON EMÍLIO SCALABRIN, PPGIa: Graduate Program on Informatics –
Pontifical Catholic University of Paraná – PUCPR
JEAN-PAUL BARTHÈS, Centre de Recherches Royallieu – Laboratoire Heudiasyc –
UTC: Université de Technologie de Compiègne
FABRÍCIO ENEMBRECK, PPGIa: Graduate Program on Informatics –
Pontifical Catholic University of Paraná – PUCPR

Finding reliable partners to interact with in open environments is a challenging task for software agents, and trust and reputation mechanisms are used to handle this issue. From this viewpoint, we can observe the growing body of research on this subject, which indicates that these mechanisms can be considered key elements to design multiagent systems (MASs). Based on that, this article presents an extensive but not exhaustive review about the most significant trust and reputation models published over the past two decades, and hundreds of models were analyzed using two perspectives. The first one is a combination of trust dimensions and principles proposed by some relevant authors in the field, and the models are discussed using an MAS perspective. The second one is the discussion of these dimensions taking into account some types of interaction found in MASs, such as coalition, argumentation, negotiation, and recommendation. By these analyses, we aim to find significant relations between trust dimensions and types of interaction so it would be possible to construct MASs using the most relevant dimensions according to the types of interaction, which may help developers in the design of MASs.

Categories and Subject Descriptors: I.2.11 [**Artificial Intelligence**]: Multi-Agent Systems

General Terms: Design, Algorithms, Security

Additional Key Words and Phrases: Trust, trust model, reputation

ACM Reference Format:
Jones Granatyr, Vanderson Botelho, Otto Robert Lessing, Edson Emílio Scalabrin, Jean-Paul Barthès, and Fabrício Enembreck. 2015. Trust and reputation models for multiagent systems. ACM Comput. Surv. 48, 2, Article 27 (October 2015), 42 pages.
DOI: http://dx.doi.org/10.1145/2816826

1. INTRODUCTION

Trust and reputation concepts are widely used in various fields of computer science, such as evaluation systems, P2P networks, grid computing, game theory, e-commerce,

Authors' addresses: J. Granatyr and O. R. Lessing, Joaquim Nabuco Street, 114, Porto União SC Brazil; emails: jonesgranatyr@gmail.com, otto@unc.br; V. Botelho, E. E. Scalabrin, and F. Enembreck, Imaculada Conceição Street, 1155, Curitiba PR Brazil; emails: {vanderson, scalabrin, fabricio}@ppgia.pucpr.br; J.-P. Barthès, UMR CNRS 7253 Heudiasyc Universite de Technologie de Compiegne BP 529 F-60205, Compiegne France; email: barthes@utc.br.

DOI: http://dx.doi.org/10.1145/2816826

semantic web, software engineering, web services, and recommendation systems [Artz and Gil 2007]. Another field in which these techniques have been gaining importance is multiagent systems (MASs), which are formed by autonomous agents that interact to achieve their own goals. To achieve their goals, agents must engage in some social activities, such as cooperation, coordination, negotiation, and conflict resolution [Wooldridge 2009]. The execution of such activities can bring many problems if agent A establishes a contract with agent B and B does not do it or executes the task dishonestly. A trusting relationship must exist between these agents when one needs to delegate a task to another. This relationship is addressed by Castelfranchi and Falcone [1998], who state that the confidence an agent has in the other's behavior is a mental attitude that will influence future decisions.

In the e-commerce scenario, the human customer can delegate the negotiation authority to his or her personal agent, who will interact and negotiate with other agents or people to reach an agreement. It is necessary to trust that the agent understands the consumer's needs and has the trade competence, ensuring that he or she will not be exploited or cheated by other agents.

In electronic auctions, bidders can collude and pay a low price for products, and afterward, they can resell them for a higher price. On the other hand, in a Vickrey auction, the auctioneer can lie to the winner about the price of the second-highest bidder, forcing him or her to pay more than he or she should [Wooldridge 2009]. As we can realize, trust plays an important role in these scenarios, and trust and reputation mechanisms were built to decrease risk in these kinds of interactions.

There are several trust definitions in the literature, and one of the most accepted is given by Gambetta [1988], who defines it as a subjective probability that an agent will perform a particular task as expected. Other authors present some variations on and additions to this definition, taking into account risk [Luhmann 2000; Castelfranchi and Falcone 2001], beliefs and dependence on actions of others [Josang 1996], and delegation [Castelfranchi and Falcone 2001]. Although there is not a consensus about the most appropriate definition, all of them follow the same base and are interrelated. Regarding implementation, trust is usually denoted by a numeric value that indicates how trustworthy an agent is, and the others take into account this value in order to decide whether or not to interact [Sabater and Sierra 2005].

On the other hand, reputation is defined as the collection of opinions received from other users [Nunes 2011] or an expectation of someone's behavior based on previous interactions indicated by others [Abdul-Rahman and Hailes 2000]. Similarly, Kreps and Wilson [1982] define it as a characteristic attributed to someone by another person or community. Mui et al. [2002], in turn, define reputation as the perception agents create through past actions about their intentions and norms, being related to expectations held of others. In the same context, Grishchenko et al. [2004] argue about expectations related to fulfillment of expected events, since these events must be similar to a past average to be considered reliable. On the other hand, Wang and Vassileva [2003] address that reputation is the belief that someone has about the capabilities, honesty, and reliability of someone based on recommendations received from others. According to these definitions, we conclude that reputation is a trust component and is also denoted by a numeric value representing the community opinion about an individual.

To construct systems based on these concepts, many researchers have developed specific architectures composed of a set of dimensions and features necessary for its operation, which we define as a trust and reputation model. In other words, a trust and reputation model is an architecture developed mainly for three proposes: (1) to extract data from the environment or from other users; (2) to use these data to compute trust; and (3) based on the calculated values, to help in decision-making processes. The study and analysis of these dimensions and features are one of the focuses of this article, and a detailed review of this topic is given in the next section.

Trust is becoming increasingly important in MAS interactions, such as coalition, competition, argumentation, and recommendation. In this context, it is necessary to know how to choose the best partners to form a team, compete with reliable agents, negotiate fair contracts with true information, or even receive recommendations on products or services according to user preferences.

As we have observed, there are several situations in MASs demonstrating that trusting relationships among agents are required. The aim of these mechanisms is to ensure security in interactions, protecting the good agents from those who may attempt to commit fraud.

There are many reviews about trust and reputation in MASs, such as the work by Pinyol and Sabater [2013], Sabater and Sierra [2005], Ramchurn et al. [2004], Lu et al. [2009], Huang et al. [2008], and Yu et al. [2013]. Each one of these papers takes into account different aspects for categorizing the trust and reputation models according to the aim of the review. Based on the analysis of the existing reviews, we have found that all papers classify the models by considering only the point of view of the concepts and principles of trust. None of the reviews focuses on the types of interaction in MASs such as coalition, argumentation, negotiation, and recommendation. The fact that most trust and reputation models are domain specific makes it difficult to select and use an existing trust and reputation model in a specific type of MAS interaction. It happens because most models are context dependent and often use particular variables from the environment. Models developed under an e-commerce scenario, for example, use variables from this environment to help in trust computation, such as price, quality, or delivery time. These variables are usually useful only in this context, since they would not be helpful in an evaluation system, where the most important variables would be the number of evaluations written or helpful votes received.

Based on these factors, this article presents a literature review that shows the trust and reputation models for MASs published over the last two decades. The first contribution is to join some of the dimensions presented by the main existing works in the field, such as Pinyol and Sabater [2013], Sabater and Sierra [2005], Ramchurn et al. [2004b], Carter et al. [2002], Lu et al. [2009], Aljazzaf et al. [2010], Grandison and Sloman [2000], Huynh et al. [2004], and Jurca and Faltings [2003]. This centralized approach provides a broad range of dimensions together in the same article, which helps when a new model is being constructed and developers are not sure about what dimensions to use, since they often do not know the existing ones in the literature. Afterward, we discuss the selected dimensions using the perspective of MASs, and we address how the analyzed models employ the concepts. Furthermore, we construct a table that provides a wide view of the most-used dimensions in MASs so we could reflect on some aspects of the relationship between trust and MAS. The table and discussions also provide a broad range of models and dimensions, so it may be useful to compare existing models.

The second and main contribution is to analyze each one of these dimensions based on the perspective of the types of interaction we have found in the MAS models, such as coalition, argumentation, negotiation, and recommendation. The objective is to find a link between trust and reputation dimensions and types of interaction in MASs so we can realize which dimensions are always present or not. This contribution can allow a future automatic generalization of trust and reputation models according to the dimensions. Additionally, we compare the models we have found in the literature with the expected dimensions a trust and reputation model for MAS should implement. In short, we define three questions we aim to answer for each one of the types of interaction: (1) What is the most common set of dimensions that has been used in the literature? (2) What are the relations of these dimensions with the type of interaction?

Table I. Existing Reviews

Sabater and Sierra [2005]	Pinyol and Sabater [2013]	Lu et al. [2009]
Paradigm type	Trust	Semantics
Information sources	Cognitive	Architecture
Visibility	Procedural	Mathematical model
Granularity	Generality	Trust network
Cheating assumptions		Reliability
Type of exchange information		Risk
Reliability measure		Dimension
Type model		
Grandison and Sloman [2000]	**Ramchurn et al. [2004b]**	
Provision trust	Individual level	
Access trust	- Sociocognitive models	
Delegation trust	- Reputation models	
Identity trust	- Evolutionary and learning	
Context trust	System level	
	- Trustworthy interaction mechanisms	
	- Reputation mechanisms	
	- Distributed security mechanisms	

(3) What are the other important dimensions not covered by the literature? When developing a new trust and reputation model for MASs, the answers for these questions will lead developers to choose the best set of dimensions according to the type of interaction, and additionally, it will help in the definition of the type of agents and relationships among them. Another useful factor of our contribution is the evaluation of existing models to verify whether it contains the necessary dimensions according to a specific type of interaction. We analyzed a total of 106 models, but a critical analysis of each one of them is out of the scope of this work. We did not do this because of the great diversity and quantity of models, as well as the dependence of context. Another reason is that we aim to identify a set of dimensions usually employed by the models so we can reflect about the recommended dimensions that should be applied to specific models and types of interaction found in MASs.

To achieve these goals, we initially selected 230 papers related to trust and reputation for MASs or intelligent agents. We later filtered the selected articles by reading their abstracts and used the following criteria for exclusion: (1) articles that were not clearly related to definition of new models, (2) trust applications in MASs, and (3) improvements or use of different algorithms in existing models. This task was accomplished by deeply analyzing each model aiming to identify the most important dimensions and types of interaction used in MASs. It is important to emphasize that reading the abstract was just a filter to select the models, which were analyzed in detail afterward.

The remaining part of the article is organized as follows: Section 2 presents the existing literature reviews in the MAS field, indicating which dimensions and features will be used in our work. In Section 3, we present the dimensional concepts as well as how the models use them in their architecture. Some discussions about MASs are also presented related to each dimension. In Section 4, we present the definitions of the types of interaction and explain how the models employ them. Additionally, we discuss the dimensions that each type of interaction should present in MASs. Finally, Section 5 concludes the article.

2. EXISTING REVIEWS ON TRUST AND REPUTATION FOR MAS

Table I shows the five reviews we used as a base in our work and the original classification proposed by their authors. These works were chosen as a base to ours because they present a considerable number of topics to be analyzed, and according to our first contribution, this represents a good opportunity to join some of them and discuss them from the perspective of MASs. Another reason to choose them is that they are the most known in the literature and they are usually used for comparisons.

Our work is different from the others for basically two reasons. The first is that the existing reviews address how the dimensions are used by trust and reputation applications in a general context, not being focused on characteristics of MASs. The second is that all reviews analyze only a few models, different from ours, which address hundreds of them, making it possible to give some basic statistics and make comparisons.

As we can observe in Table I, each one of the five literature reviews takes into account different aspects to categorize the models, and the authors define a set of characteristics aiming to indicate how the models employ such concepts. Besides them, other reviews focused on MASs have been reported by Huang et al. [2008] and Yu et al. [2013]. The former takes into account the trust management process, while the latter is focused on the load balancing among high-reputation agents, which is addressed in SecuredTrust [Das and Islam 2012]. No dimensions are used from these reviews because they do not actually present ways for comparison.

We did not consider all the dimensions proposed by the authors because some of them are repetitive among the papers or they are not applicable to our study. For example, we did not use the *type of exchange information* dimension from Sabater and Sierra [2005] because it is related to the type of information transmitted by agents when they use witness information, and according to Pinyol and Sabater [2013], it would be necessary to provide more details for a better understanding nowadays. The *type model* dimension is also not considered, and the reasons are addressed by Pinyol and Sabater [2013] and are discussed later in this article, in Section 3.12. Apart from these two features, all other dimensions were included in our discussions.

From Pinyol and Sabater [2013], we discuss in this article only the *trust* dimension because it presents a way to indicate if models are really trust models according to the arguments from Castelfranchi and Falcone [1998] (Section 3.12 discusses this issue). The *cognitive* dimension was not included because it only indicates if models do or do not present cognitive essence, differently from the *paradigm type* from Sabater and Sierra [2005], which indicates if models do or do not present numerical or cognitive essence. We decided to use the *paradigm type* from Sabater and Sierra [2005] because it presents more details to classify models. Similarly, the *generality* dimension was also not included because it is equivalent to *granularity* from Sabater and Sierra [2005]. Finally, *procedural* was also not discussed in our work because it only indicates if models clearly present implementation details. It was not included because it does not present ways to compare or classify models.

From Lu et al. [2009], we discuss only the *semantics* and *risk* dimensions because both of them are considered trust principles by Aljazzaf et al. [2010]. We did not include *architecture, reliability,* and *dimension* because they are respectively equivalent to *visibility, reliability measures,* and *type model* from Sabater and Sierra [2005]. On the other hand, the *mathematical model* dimension aims to indicate the equation used to compute trust or reputation, and it was not included because it also does not present ways for classifying or comparing models. Finally, the *trust network* dimension aims to study the topology used to organize witnesses, and we decided not to include it because trust network is a technique used to collect witness information, which is discussed in this article in Section 3.2.3.

From Grandison and Sloman [2000], we discuss only the *delegation trust* dimension, which is also addressed by Castelfranchi and Falcone [1998] as an important trust aspect. The other dimensions from this review were not included in our work because they do not present ways to compare and classify models. For example, *provision trust* is related to trust in services, *access trust* deals with assessment of resources, and *identity*

Table II. Our Dimensions

Dimension	Values
Par - Paradigm [Sabater and Sierra 2005]	N - Numerical C - Cognitive
InS - Information sources [Sabater and Sierra 2005; Carter et al. 2002; Huynh et al. 2004]	DI - Direct interaction [Sabater and Sierra 2005] DO - Direct observation [Sabater and Sierra 2005] WI - Witness information [Sabater and Sierra 2005] SI - Sociological information [Sabater and Sierra 2005] P - Prejudice [Sabater and Sierra 2005] CR - Certified reputation [Huynh et al. 2004] RL - Rules [Carter et al. 2002]
Che - Cheatings assumptions [Sabater and Sierra 2005]	L0 - No cheating L1 - Bias information L2 - Cheating
Smn - Trust semantics [Lu et al. 2009; Aljazzaf et al. 2010]	- - No √ - Yes NA - Not applicable
Prf - Trust preferences [Aljazzaf et al. 2010]	
Dlg - Delegation trust [Grandison and Sloman 2000]	
Rsk - Risk measure [Lu et al. 2009]	
Fdb - Incentive feedback [Jurca and Faltings 2003]	
Int - Initial trust [Aljazzaf et al. 2010]	
Ope - Open environment [Huynh et al. 2004]	
Hrs - Hard security [Ramchurn et al. 2004b]	

trust approaches access control. Finally, *context trust* is equivalent to the *granularity* dimension presented by Sabater and Sierra [2005].

From Ramchurn et al. [2004b], we address only the *distributed security mechanisms* from the *system level*, which we refer to as *hard security* in this article. As we can observe in Table I, this review focuses on the individual level and system level. The former is related to beliefs about the honesty of interaction partners, while the latter focuses on protocols or mechanisms that regulate the system. We did not include the other dimensions because they do not present ways for comparisons.

In addition to these reviews, we will also use in our work concepts such as initial trust [Aljazzaf et al. 2010], preferences [Aljazzaf et al. 2010], open environment [Huynh et al. 2004], and incentive feedback [Jurca and Faltings 2003]. These dimensions were added in our work because we have found that some analyzed models discuss these topics and are in fact considered trust principles by Aljazzaf et al. [2010].

Table II shows a complete list of all dimensions used in our review. The first column indicates the names of the dimensions, while the second presents their values. As discussed earlier, we did not classify the models according to all features presented in Table I, as we argue that not all of them are dimensions of the models. We have also added two more information source values, extending the original review by Sabater and Sierra [2005]. The additional values are certified reputation [Huynh et al. 2004] and rules [Carter et al. 2002], and they are considered as information sources because they represent ways to extract information from the environment to construct trust.

Based on Table I, it is important at this point to differentiate between what we consider as dimensions and characteristics of the models. Dimensions are related to the way the model is defined, such as its internal architecture. It must be taken into account when building, evaluating, or comparing models. On the other hand, characteristics are related to implementation aspects and particularities of the models. Some examples are *visibility* [Sabater and Sierra 2005; Lu et al. 2009], *granularity* [Sabater and Sierra

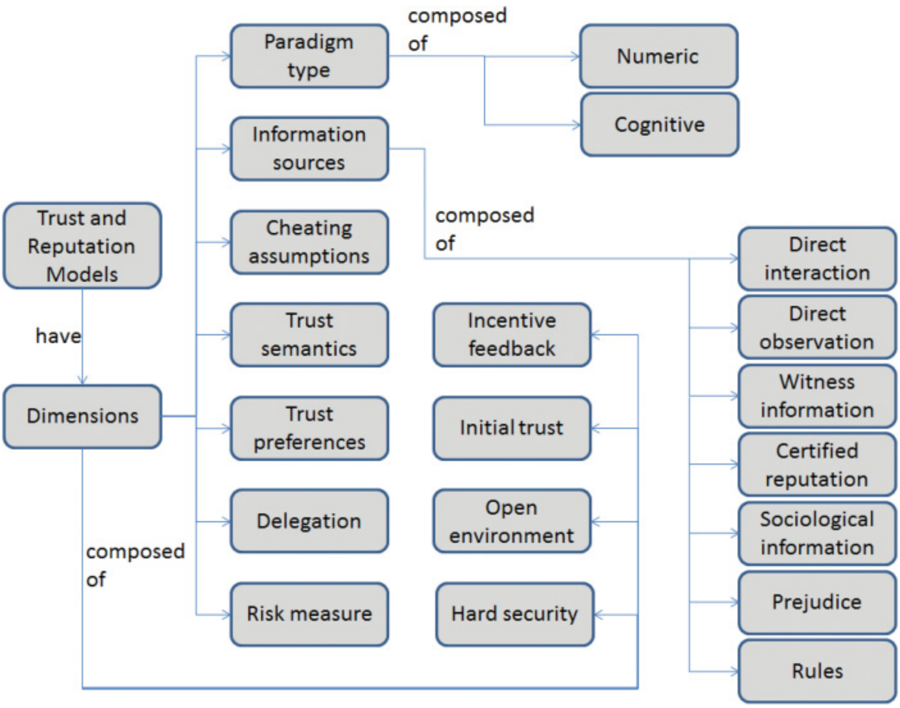

Fig. 1. Dimensions of trust and reputation models.

2005; Pinyol and Sabater 2013], *reliability measures* [Sabater and Sierra 2005; Lu et al. 2009], and *trust* [Pinyol and Sabater 2013]. Although they are not directly related to architecture, these features are important components and they are briefly discussed in Section 3.12 later in this article. Figure 1 shows a conceptual view of the dimensions used in our work.

As we can observe in Figure 1, trust and reputation models have a set of dimensions, while some of the dimensions are composed by a set of values. In short, this figure exemplifies what we consider as a trust and reputation model.

3. TRUST DIMENSIONS

Based on the dimensions shown in Table II, the aim of this section is to define each one of them and show how trust and reputation models are related to them. This section presents our first contribution, including explanations about how MASs make use of these dimensions and a general discussion about all the dimensions used in the literature.

3.1. Paradigm Type

The paradigm type is related to the method used to build the model, and it can be classified as cognitive, numeric, or hybrid [Sabater and Sierra 2005].

The cognitive paradigm is related to beliefs and mental states agents have. Trust is measured by the degree of these beliefs and the mental consequences of the decision to trust or not to trust another agent. This paradigm is linked to cognitive architectures and it is closer to the BDI (believe, desire, and intention) agents [Sabater and Sierra 2005]. In other words, cognitive models are built to equip machines with the closest human behaviors using human cognitive processes to calculate trust.

The first cognitive model was proposed by Castelfranchi and Falcone [2001], and it is based on trust as a result of a mental state composed by some cognitive components, such as objective, ability, competence, and dependence. Another example is the model proposed by Neville and Pitt [2004], which is based on the social theory of trust, reputation, recommendation, and learning through direct experiences integrated in the agent reasoning mechanism. The model by Carter and Ghorbani [2003] takes into account the combination of self-esteem, reputation, and familiarity among the agents, while Zhang et al. [2007] argue that intimacy directly influences trust. The authors use human feelings for partner selection.

Similarly, the model by Sutcliffe and Wang [2012] uses Dunbar's Social Brain hypothesis [Dunbar 1998] to introduce friendship concepts such as best friends and casual friends. This model is based on trust expression through emotions, which is also addressed by Pinto [2008], where he uses concepts of weak and strong personalities integrated into emotional states, such as happiness and sadness. In this model, strong personality agents have more influence on others, while weak personality agents are submissive to others. The model by Singh [2011] uses the BDI architecture to support intuition and the semantic concept of a rich vocabulary to represent the evaluations. Carbo et al. [2002] propose a trust model applied to e-commerce, and they introduce the hierarchical layers of the interaction concept. The mental model represents behaviors such as selfishness, sociability, and susceptibility. The social model stores the desire of isolation, and the world model contains the interaction rules to be used among agents. These rules are defined when agents request recommendations or when they respond to certain requests.

The BDI + Repage model [Pinyol et al. 2012] includes concepts of image as a composition of the set of beliefs that are based on specific goals independent of the reputation value. An agent may have a low reputation value related to a certain dimension, but its image may be good for other agents who see it from another perspective. On the other hand, the model by Chopra et al. [2011] deals with the integration of technical and cognitive trust. Other examples about cognitive architectures are the models by Piunti et al. [2012], Venanzi et al. [2011], and Castelfranchi et al. [2003], which are all based on the trust theory of Castelfranchi and Falcone [2001], and cognitive maps are used as the agent reasoning mechanism.

On the other hand, the numerical paradigm does not use cognitive representations, and it is closer to reactive architectures. It is based on the numerical aggregation of past interactions and presents a set of subjective probabilities that agents will correctly perform a given task [Sabater and Sierra 2005]. Almost all numerical approaches use statistical methods to compute trust, and they commonly employ Bayesian probabilities [Regan et al. 2006; Teacy et al. 2012; Fang et al. 2012], fuzzy sets [Schillo et al. 2000], probability distribution [Sen and Sajja 2002], and Dempster-Shafer functions [Yu and Singh 2003; Liu et al. 2012]. Machine learning is also used in the works of Tran and Cohen [2004] and You [2007], which propose reputation algorithms using reinforced learning.

Hybrid approaches that use both paradigms are also present, such as the work by Matt et al. [2010], Bentahar et al. [2007], Koster et al. [2011], and Parsons et al. [2011]. These models are cognitive because they are based on beliefs and numerical because they use numerical aggregations. In Section 4.2, the details about these models are presented.

It is possible to coexist on the same MAS numerical and cognitive agents, considering the needs of each paradigm. Numerical agents expect to find in the environment objective data that may be applied in mathematical equations, while cognitive agents usually expect subjective or complex information from the environment. As an example, if an MAS will be developed for the stock trader scenario using a hybrid approach, it would be necessary to provide a set of numbers related to purchase and sales transactions, as well as analytical reports about companies and the market.

3.2. Information Sources

To calculate trust and reputation values, agents need to extract data from other agents or from the environment. There are several ways to do it, and they are explained in the next sections. It is important to emphasize that not all of them will be implemented by all agents in the same MAS, since it will depend on the type of application and the agent's architecture.

3.2.1. Direct Interaction. Direct interaction occurs when agent *A* needs to interact directly with agent *B* to be able to evaluate the transaction. An example is the purchase of a product, where the agent needs to acquire the product and the transaction is afterward evaluated. Direct interaction is considered the most relevant information source, but many interactions are required to have a great amount of reviews [Sabater and Sierra 2005].

The Marsh model [Marsh 1994] is one of the first computational trust models in the literature and is characterized by the use of only direct experience to estimate agents' reliability. Similarly, MDT [Griffiths 2005] only takes into account this information source to select partners for task delegation, while the model proposed by Ghanea-Hercock [2007] uses it to choose the best partners to form coalitions.

There are few models that employ only direct interaction, and we realize that the majority use this information source combined with others. As mentioned earlier, it happens because many interactions with the same agent are necessary to achieve high levels of trust, and this fact is not viable in all kind of applications, mainly in MASs. A classic scenario explored by many MASs is the Prisoner's Dilemma [William 1992], in which two prisoners are induced to betray each other to reduce their own prison sentence. Direct interaction between prisoners can be addressed by a trust model that takes into account the results of previous iterations. An example that uses this scenario is the model by Schillo et al. [2000].

As the tendency of MASs is to be open, direct interaction on its own is insufficient for applications in this type of environment, requiring other mechanisms to compute trust. The following sections present some other alternatives that can be used in combination with direct interaction.

3.2.2. Direct Observation. Direct observation is based on the observation of others' interactions to analyze their behavior [Sabater and Sierra 2005]. Differently from Section 3.2.1, there is no interaction between agents to compute trust, and when agent *A* wants to buy a product from agent *B,* direct interaction is not necessary. Instead, agent *A* will observe agent *B*'s behavior in past or current interactions and make a decision about interacting or not.

The works by Carter and Ghorbani [2003], Rettinger et al. [2008], Sierra and Debenham [2005], and Klejnowski et al. [2010] perform direct observation through characteristics perceived in a trust situation, such as the amount of feedback provided by agents, the percentage of positive reviews, prior actions, the roles related to agents, and the results of contracts. Similarly, the model by Teacy et al. [2008] aims to observe the result of services rendered by agents, updating agents' beliefs about the service provider.

The models by Rehák et al. [2005] and Zheng et al. [2006] propose utility functions used in their past interactions to evaluate and select partners, while Schillo et al. [2000] present how direct observation can be shared among agents in negotiation scenarios in e-commerce. Serrano et al. [2012] proposes the analysis of ACL (Agent Communication Language) messages within the MAS to extract data that can characterize agents' trust. They use machine learning, and trust is defined according to the conversation model among agents.

As this information source allows observation of the information exchanged among agents, it is necessary to build security mechanisms preventing the exposure of the observed agents, such as hard security techniques. Salehi-Abari and White [2012] implement the concept of neighbors' agents, which allows the observation of direct interaction only by the confident neighbors.

Unlike direct interaction, this information source can be better applied to MASs because, as there might be many agents in the environment, it cannot be viable to interact with most of them due to performance problems.

3.2.3. Witness Information. Witness information is commonly used when agents do not have direct information and they need to ask other agents about the trust of the target. When agent A needs to interact with agent B and there is no direct interaction between them, agent A can query agent C to obtain his or her opinion about agent B. It is important to emphasize that agent C must have had direct experience with agent B. This method is also known as indirect information or reputation [Sabater and Sierra 2005], and it is calculated through the aggregation of opinions from agents who have had some interaction with the trustee.

There are two types of information sources in this category: (1) simple transmission of reports and (2) recommendations or opinions. In the first case, the witness reports are queried through the consultation of agents, but it is not important to select the best ones to obtain information. Some examples are BRS [Josang and Ismail 2002] and TRAVOS [Teacy et al. 2006]. On the other hand, a recommendation or opinion is an evaluation coming only from agents that are already trusted in a relationship network built by the agent itself [Montaner et al. 2002]. This network is called Trust Net and is addressed by Yu and Singh [2003]; it allows the assessment of the honesty of witness-based observations based on evidence theory to calculate the possibility of a witness sending false reports. Other related examples are TRUMMAR [Derbas et al. 2004] and Wang and Zhang [2005].

In the work presented by Wang and Gui [2013], recommendations are addressed using the information entropy theory, which is concerned with the loss of the meaning of information between agents. The model also proposes evaluation of recommendations based on two approaches: (1) the proximity of the nodes between the witnesses and (2) the similarity of the reviews' content.

Similar to direct interaction, this information source is often combined with others, and there are few models that make use of only this technique. An MAS application that usually takes into account only this type of information source is recommender systems, which aim to search for information about products or services for users based on the information of others [Montaner et al. 2002; Bedi et al. 2007; Song et al. 2004]. This kind of recommendation will be explained later in this article, in Section 4.4, and some MAS examples will be presented. Other examples are the pure reputation system, which uses only information from testimonies, and some works are the models proposed by Koster et al. [2011], Parsons et al. [2011], Bertocco and Ferrari [2008], Elgohary et al. [2010], Liu et al. [2012], Liu et al. [2011], and Liu et al. [2013a].

3.2.4. Certified Reputation. Certified reputation occurs when the evaluated agent has a list of other agents who can testify about him or her. When agent A evaluates agent B, B locally stores a reference of A as a witness. If another agent needs to interact with B's witnesses, it should perform a direct query to B. It is used as a shortcut to obtain a relevant set of witness information using few interactions. In other words, certified reputation is considered a recommendation letter from an employer about an employee. In this context, the employer will register its recommendation and the letter will contain all the information about the employee [Huynh et al. 2006; Huynh et al. 2004]. The set of letters will be used whenever someone asks for information about the employee.

The FIRE model [Huynh et al. 2004] implements certified reputation as part of trust computation, and its greatest benefits particularly affect the first interactions among agents. Similarly, the model by Huynh et al. [2004] also uses this information source. On the other hand, the model by Botelho et al. [2009] widens the certified reputation concept by adding the storage information about witnesses and the ratings received by them. It is possible to calculate reputation using a single query to the agent reported. To prevent fraud, the authors implement encryption and digital signature, which are necessary because the set of evaluations is in the possession of the evaluated agent and can be easily modified by malicious agents if this mechanism were not implemented.

To employ certified reputation in MASs, the model must deal with dishonest manipulation of the list of witnesses the agents hold. If this issue is solved, the main benefit of certified reputation would be the low cost to find witnesses, which is in fact a performance problem that usually occurs on models that use indirect information to compute trust.

3.2.5. Sociological Information. This type of information source relates to the social relationship among agents and their roles in the community, which influences relationships with others. Similar to direct interaction, there must be many interactions between agents because it requires social network analysis [Sabater and Sierra 2005].

One of the most popular models that uses these concepts is Regret [Sabater and Sierra 2002], which implements graphs called sociograms to indicate the relationship among agents. Sociograms group agents to get information from those who are more representative. The models by Sutcliffe and Wang [2012] and Liu and Datta [2012] show how the trust formation process is achieved through social structures based on friendship, familiarity, and camaraderie. The work by Klejnowski et al. [2010] focuses on the trusted community concept using adaptive agents, since high degrees of confidence are expected from members belonging to the same community. Similarly, TRUMMAR [Derbas et al. 2004] collects information using a trust hierarchy formed by strangers, friends, and neighbors on mobile agents, while Li et al. [2007] use a network of agents to search for evidence that can provide references for partner selection.

StereoTrust [Wang and Gui 2013] is inspired in real stereotypes, which represents characteristics and expected behaviors of agents. This model measures the confidence of unknown agents by the observation of similarities and differences between them. Another approach is the work by Ashri et al. [2005], which identifies relationships among agents and the types of relationships that may be considered as reliable. In this model, ontologies are used to interpret the significance of the relationships. On the other hand, DiffTrust [Fang et al. 2013] considers identity and status to evaluate the agent's position in the social network, while in the MAS by Salehi-Abari and White [2012], agents have different society roles and their judgment is made based on their roles and relationships with other roles presented in the environment.

3.2.6. Prejudice. Prejudice consists of signs that identify the individual as a member of a group, such as skin color, religious beliefs, uniform color, previous workplaces, educational qualifications, and hobbies, among others [Sabater and Sierra 2005]. These features are context dependent, since each type of environment will need different variables.

The model by Burnett et al. [2013] uses observation of characteristics to build stereotypes of agents, which are used when direct or indirect information is not available on the system. These features are dynamically built based on agents' experience in executing tasks, and this is done through the use of machine-learning techniques. Similarly, the model by Liu and Datta [2012] discusses the concept of an agent's profile, which is constructed by collecting basic data from individuals, such as age, gender, and location. FOCET [Mokhtari et al. 2011], in turn, takes into account cultural aspects, language, nationality, and morality.

On the other hand, the work by Ramchurn et al. [2004a] presents an institutional approach, whereas agents that belong to powerful groups (legal institutions, the government) have more credibility than agents belonging to weaker groups, such as small companies or individuals. Regret [Sabater and Sierra 2002] incorporates the system reputation concept, which allows the definition of initial trust based on institutional structures.

The use of ontology is an interesting way to develop MAS based on prejudice, since it may enable dynamic support about new concepts that appear in the environment. For example, when new agents arrive in the community, new prejudices can be introduced, especially in open environments.

3.2.7. Rules. Rules are predefined social norms within the model and they are similar to the concept of system reputation proposed in Regret [Sabater and Sierra 2002]. They are used to standardize agents' behaviors, preventing them from acting differently from the rules. As an example, the model by Carter et al. [2002] evaluates reliability through four basic concepts: (1) interactivity, (2) content provision, (3) feedback, and (4) longevity. The interactivity role is related to the regular use of the system, so the agents must be interacting to keep it continuously up-to-date. Content provision concerns the constant production of content in the system, while feedback aims to incentivize agents to provide quality feedback information using testimonies. Finally, longevity is related to maintenance of a high reputation in the whole system to promote its durability. To compute trust, these four rules are combined and the result value is measured by the observation of the obedience to them.

The work by Hermoso et al. [2010] focuses on the automatic creation of roles using the *k-means* algorithm for clustering and creation of taxonomies that show agents' confidence. In this way, rules associated with agents generate expectations about their behavior or capacity. The FIRE model [Huynh et al. 2004] uses similar concepts and it employs rules that define the minimum quality of products to be sold. Thus, all seller agents must follow this rule and they cannot sell products with a quality below the threshold defined in the system. The model by Nkosi et al. [2007] is similar, and it deals with interaction rules for communication in mobile agents. The ASC-TMS [Yaich et al. 2011] defines user and community policies, so agents in the environment must follow it to ensure its reliability. FOCET [Mokhtari et al. 2011] includes a set of public rules that must be respected, while Urzica [2010] presents a mechanism to collect and associate roles to agents in the environment.

The model by Chopra et al. [2011] deals with Sociotechnical Systems (STSs), which are complex structures composed by humans, organizations, and their information systems. They address how an STS should be modeled to guarantee trust relations, and roles are used to evaluate if a system is more trustful than another one based on particular roles' perspectives. In other words, developing trustful STSs implies a reasoning process about role-based perspectives and the establishment of commitments among agents that adopt different roles.

Rules such as feedback can be dealt with by agents themselves, since the agent can manage the reports given to others. However, other rules need the support of the MAS's architecture, such as the interactivity rule among agents. In this sense, the model by Botelho et al. [2009] uses the *time* concept, which stores the times the interactions happened, aiming to measure the frequency of interactivity. As we can realize, this variable is controlled by the MAS itself.

As we could observe in the last sections, information sources are also related to data that agents extract from the environment. Rules fall into this category because agents need to get information from the predefined norms existing in the architecture to make a decision. For this reason, rules are considered an information source.

3.3. Cheating Assumptions

This dimension is related to the ability agents have to identify fraud in communication. Sabater and Sierra [2005] defined three levels: 0, 1, and 2. Level 0 is related to models that do not consider fraudulent information and they do not present mechanisms to filter malicious agents.

Level 1 is applied to models that consider biased information; for example, agents can hide information but they do not lie. In this context, important data can be lost if biased or incomplete information is ignored, and PRrep [Haghpanah and desJardins 2012] addresses this issue by focusing on the use of biased data through Bayesian learning. To check the reliability, the model compares this data to direct experience already existing on the system.

Level 2 is related to models that employ mechanisms to detect cheaters. LCCM [Tong et al. 2009] can prevent cheaters from using personalized information about agents, while SecuredTrust [Das and Islam 2012] states that good agents always send trustful information and bad agents always send false information. However, in a real scenario, good agents can transmit false data to their competitors, and bad agents can occasionally send reliable information to hide their true nature. Based on this, SecuredTrust [Das and Islam 2012] presents similarity functions that are used to identify false reports that take into account agents' credibility. Another example is TRAVOS [Teacy et al. 2006], which uses probability functions to estimate if the information sent by agents is reliable. This is performed by comparing previous interaction results with current information, and if there is no similarity between the compared information, it means the probability that the report is false is greater.

DiReCT [Aboulwafa and Bahgat 2010] and Liu and Datta [2012] compare received recommendations with the agents' own opinions about the recommendation. According to similarity between recommendations and opinions, agents can decide whether to consider the information received important. iCLUB [Liu et al. 2011], in turn, collects testimonies, groups them into clusters, and performs an intersection calculation between the generated clusters to compute trust. Salehi-Abari and White [2012] address attacks from malicious agents when they try to unduly improve their reputation, alone or in a group of agents working collaboratively. The authors present an approach they consider as a new information source called *reporting interaction*, which provides a distributed mechanism to disseminate information in the environment.

There are other models that evaluate whether there are cheater agents in the environment, and most of them employ similar techniques to those described earlier. When developing MASs, mechanisms to prevent cheating must be implemented, since the origin and intentions of agents are often not known, especially in open environments.

3.4. Trust Semantics

Most models measure trust only taking into account one single value, which indicates whether the agent is or is not reliable. On the other hand, semantics or multidimensionality aims to transform this single value in an average of several aspects, converting it into a composite measure [Lu et al. 2009; Aljazzaf et al. 2010].

Regret [Sabater and Sierra 2002], Bertocco and Ferrari [2008], and Wang and Zhang [2005] are examples of models that use ontologies to combine different aspects into one single value. Regret [Sabater and Sierra 2002] presents a seller ontological structure defining the weights 0.6 for product delivery and 0.4 for product quality. These measures are combined to create the semantic dimension, and agents can decide which feature is the most important according to his or her needs. The Priority-Based Trust Model [Su et al. 2013] measures trust through adjustable priority sets according to agents' preferences. In this model, priority is assigned to agents by the definition of weights into factors, such as cost, speed, and quality.

There are other works also implementing the semantic dimension. However, instead of using ontologies, they use simple numeric values. The model by Matt et al. [2010] presents some attributes that agents must be in accordance with to obtain a good review, and some examples are availability, security, privacy, and reliability. Klabi et al. [2012] argue that negotiation processes cannot only have a single value, and they define some criteria, such as investment value, price, utility, and sensibility. Similarly, MDT [Griffiths 2005] is focused on task delegation, and weight functions are used to measure time, quality, and cost to construct the final trust value.

Other models that use semantics are similar to those described previously and they present only differences in the variables to be considered in trust calculation. It is important to the architecture of MAS to clearly represent the way the evaluations are displayed, so all agents can interact coherently using the same semantic standard. Any semantic distortion may compromise the reliability of the results about trust calculations, and to deal with this issue, the use of ontologies provided by the MAS can be an alternative to all agents in the environment evaluating their partners correctly.

3.5. Trust Preferences

As discussed in Section 3.4, the semantic model allows trust representation through some factors related to a particular application. On the other hand, preferences are related to the possibility agents have to define weights for each attribute according to its needs [Aljazzaf et al. 2010].

Koster et al. [2011] implemented a priority system in which agents can define the most important aspects related to their goals. For example, if the product price is more important than delivery time, a rule is created based on this preference. Similarly, MDT [Griffiths 2005] uses a weighting function to select the most representative attributes in task delegation, such as quality, cost, and degree of success.

In most cases, models that allow preference selection are directly related to the semantic dimension. However, DiReCT [Aboulwafa and Bahgat 2010] permits the definition of weights to direct interactions and witness information by the user. This mechanism is useful when there is no sufficient direct information and it is plausible to provide greater weight to indirect interactions, such as witness information or certified reputation. CRM [Khosravifar et al. 2012] does so in a similar way, allowing agents to define weights between recent and old interactions. Wang et al. [2008], in turn, report a mechanism where agents can customize their behavior based on the risk of interaction. FOCET [Mokhtari et al. 2011] is focused on context construction and allows agents to choose preferences on context usage and evaluations. Finally, the model by Montaner et al. [2002] proposes a trust model used in recommender systems where agents have preferences on products according to user needs.

Preferences are often a kind of information managed internally by the agent itself, so it is important to model MASs to include mechanisms that facilitate the system priorities and agents' preferences. To deal with this issue, ontologies could be used to represent agents' preferences, so it would be easy to share these concepts with the rest of the community. MASs can represent preferences in data structures in which the weights are recorded at the end of each interaction.

3.6. Delegation

Trust and delegation concepts in MASs have been introduced by Castelfranchi and Falcone [1998], who argue that trust is necessary in task delegation. This concept is also discussed in the review proposed by Grandison and Sloman [2000], and they argue that cooperation and delegation are key features in MASs. The MDT [Griffiths 2005] model has been designed to work with task delegation, and a grid-computing scenario is presented. Each agent has (1) a set of capabilities visible to others and (ii) a set of tasks that must be accomplished using cooperation. The objective is to determine the best partner to delegate a task to based on agents' preferences and capabilities.

Burnett et al. [2011] propose a payment function that specifies the compensation the agent will have depending on the outcomes of delegated tasks. Agents can choose five different strategies to delegate, such as simple delegation, monitored delegation, nonmonitored delegation, incentive delegation with reputation, and withdrawal of delegation. Chopra et al. [2011] developed *trust-supporting mechanisms* (delegation, compensate, undo, and renegotiate) in their model, which are used to influence positively other trust relationships. They argue that delegating responsibilities makes the relation among users more robust and trustful. Additionally, they also deal with *redundancy*, which is another trust mechanism they consider to be a special case of delegation.

Other models that implement delegation concepts are the ones by Carter and Ghorbani [2003], Neville and Pitt [2004], Burnett et al. [2013], Piunti et al. [2012], and Venanzi et al. [2011]. All of them are not specific on this task and they do not have many details about how this process happens.

3.7. Risk Measure

Trust is only required in risk situations when agents have something to lose if trust is violated [Aljazzaf et al. 2010]. Daignault et al. [2002] argue that risk is the core of trust, and according to Lu et al. [2009], it is also necessary to use risk management in trust and reputation models to monitor environmental changes. Additionally, it is important to calculate risk measures before interaction with another agent, especially in situations where task delegation is necessary.

Castelfranchi and Falcone [2001] address this fact in an abstract way regarding the risks of failure, frustration, and effort loss when an agent trusts another, especially in delegated tasks. In a pragmatic way, Wang et al. [2008] use risk measures employed by utility functions that are based on agents' personal attitudes toward risk. This function returns the uncertainty degree about the interaction and it is used by agents to make a decision before interacting with others. The model by Ramchurn et al. [2004a] uses probabilities to estimate risk through functions that estimate the agent utility loss. If the function returns a high value, the risk of interaction is also high.

Other models that present characteristics related to risk are the ones by Rehák et al. [2005], Burnett et al. [2011], Marsh [1994], and Venanzi et al. [2011].

3.8. Incentive Feedback

One of the problems related to models that make use of witness information is that agents have no interest in cooperating or in providing true information about its interactions. This happens because when agents tell the truth, they are increasing the competitiveness of others. On the other hand, if agents report false information, they are decreasing competitiveness and increasing their own reputation [Jurca and Faltings 2003].

To deal with this issue, the model proposed by Jurca and Faltings [2003] defines the concept of broker agents, called R-agents, who buy and sell reputation information.

Using this mechanism, agents must provide their feedback because otherwise, they will have no money to buy witness information. In the model by Wang and Zhang [2005], agents' reputation is increased when they provide useful references, while reputation is decreased for bad agents. Another approach is the model by Carter et al. [2002], where an administrative feedback role is defined and agents must always provide information about their interactions, but an agent's trust value is decreased if it is not respected (Section 3.2.7).

3.9. Initial Trust

According to duPreez [2009], trust is composed of three distinct phases, starting from the initial setting up of trust and ending with trust dissolution over time. Aljazzaf et al. [2010] state that in most studies, it is assumed that trust already exists. However, it is necessary to initialize the initial value of agents who have just entered the system basically for two reasons. The first reason is that new agents cannot be hampered because of lack of evaluations, while the second reason is that agents that already belong to the environment cannot be cheated by the new ones. Moreover, Barber et al. [2003] argue that one of the major difficulties in developing trust and reputation models is the setting up of initial trust to newcomers.

With respect to this issue, IRTM [Rettinger et al. 2007] focuses on initial trust building, especially in open environments where agents are unknown. The model uses machine learning to predict trust values associated with the expectations of future actions in a given context. Burnett et al. [2013] use prejudice information in the form of stereotypes to provide initial trust to newcomers, while the recommender system developed by Montaner et al. [2002] also applies machine learning to generate an initial profile for agents that recommend information about products. In the models by Regan et al. [2006] and Muller and Vercounter [2005], reputation values are in the range of -1 and 1. It means that negative values represent distrust, positive values represent trust, and newcomers have the initial value set to 0, which represents a neutral position. The model by Yu et al. [2008] uses fuzzy calculations based on confidence level and system conditions, while Shi et al. [2005] estimate initial trust through a Bayesian probability distribution based on information about the environment. Similar models are the ones proposed by Rettinger et al. [2008], Derbas et al. [2004], and Sharma et al. [2012].

On the other hand, Regret [Sabater and Sierra 2002] and Hermoso et al. [2010] use roles to assign initial trust values to new members. According to these authors, these techniques are useful when agents have no interaction and they must have some information about other agents to estimate initial trust. In the same context, DiffTrust [Fang et al. 2013] analyzes agents' proximity in the social network to compute initial trust, so this value is assigned related to its closest neighbors in situated MASs.

We did not include in this dimension models that assign random values to newcomers, such as Josang and Ismail [2002], Aboulwafa and Bahgat [2010], Das and Islam [2012], Mui [2002], and Rubiera et al. [2001].

3.10. Open Environment

Open MASs are systems where agents belonging to different groups and provided with all types of interests can join and leave the system at any time. Agents are often uncertain and do not know everything about the environment, and it is impossible to control them using a central authority [Huynh et al. 2004]. For this reason, trust in this kind of environment is seen as a critical problem.

According to Huynh et al. [2004], three characteristics are relevant to a trust model that intends to deal with this kind of environment: (1) present different information sources in the sense that if one of them are out, other can be used instead; (2) be decentralized, so each agent has its own evaluation mechanism; and (3) be robust against cheater agents because each one is self-interested. Models that use certified reputation [Huynh et al. 2006; Huynh et al. 2004; Botelho et al. 2009] are examples of the first characteristic because the evaluations are stored in the agent's own database. With this information source, if the evaluator is no longer in the system, the review will remain available.

CRM [Khosravifar et al. 2009] implements the third characteristic and has mechanisms to estimate ratings in an offline manner; that is, after the agent has made a rating, the model compares it with the opinions of others to deduce the noise within the system. Similar models are the ones proposed by Teacy et al. [2008], Liu and Datta [2011], and Teacy et al. [2006]. FOCET [Mokhtari et al. 2011] makes context representation using ontologies, and agents are capable of defining weights to adjust the environmental changes. Other models that use context information in open environments are the ones by Liu and Datta [2012], Wang et al. [2008], Rettinger et al. [2008], and Rettinger et al. [2007].

There are other approaches to deal with information in open environments. For example, Burnett et al. [2013] use stereotypes, Hermoso et al. [2010] apply roles, and Burnett et al. [2011] focus on task delegation. On the other hand, Sutcliffe and Wang [2012] and ASC-TMS [Yaich et al. 2011] are focused on social agents in virtual communities.

An essential requirement to design open MASs is the ability to identify agents entering the system. This mechanism is necessary because, as they can freely enter and leave the system at any time, it is important to avoid bad-reputation agents from coming again using new credentials aiming to delete their past behavior or using the credentials of others. An alternative to deal with this issue is the use of digital certification to correctly recognize agents, which is not employed by these models.

3.11. Hard Security

When developing security mechanisms in software systems, basically two approaches can be used: hard security and soft security. Hard security consists of the standard techniques widely used in software systems, such as identity, integrity, privacy, and authenticity, usually implemented by cryptography and policies. On the other hand, soft security mechanisms consist of trust and reputation techniques related to the logical protection of the system, based on observations of others' behaviors. Based on that, the aim of this section is to present trust and reputation models that also include hard security along with soft security.

One of the dimensions presented in the review by Ramchurn et al. [2004b] is the *system level*, which is composed of rules, policies, and security mechanisms and related to hard security techniques. It is important to keep these mechanisms in MASs because hard security is an important feature in this type of application [Aboulwafa and Bahgat 2010]. However, as discussed by Blaze et al. [1999] and Finin and Joshi [2002], security techniques commonly used in distributed systems (hard security) are not totally suitable for MASs because a distributed system does not have the same flexibility as agent-based systems. This is one of the reasons for the widespread use of soft security mechanisms in MASs.

In this context, the DiReCT model [Aboulwafa and Bahgat 2010] presents a complete mechanism composed of credentials and permissions for MASs. The reputation approach of this model is combined with the hard security mechanism, which provides integration of soft and hard security. In this way, agents need a combination of both factors to access the system, such as a good reputation (soft security) and credentials (hard security). The models by Huynh et al. [2006], Botelho et al. [2009], and Borrell et al. [2001] employ digital signature to ensure authenticity and confidentiality of reports provided by agents. Authenticity is determined by digital signature, since the hash of the evaluation is encrypted using the private key of the evaluator agent. Thus, only individuals with the public key of the evaluator will be able to decipher the hash of the review, which guarantees that the recipient is who he or she claims to be. Confidentiality is used by Padovan et al. [2001], and it allows evaluations to be sent only to interested agents presenting on the content of the messages. In this situation, evaluations are encrypted using the public key, and only the recipients will be able to open it. Similarly, in the model by Jurca and Faltings [2003], agents need to send the encrypted evaluations to a central entity using public and private keys. Finally, the models by Nkosi et al. [2007], Bertocco and Ferrari [2008], and Biyela [2004] implement authentication to guarantee access security.

3.12. Other Characteristics

As discussed in Section 2, in this part of the article we will briefly explain some other characteristics that are relevant to the models but that we do not consider as dimensions.

The first one is *visibility* and it is classified as subjective and global. Subjectivity is used by decentralized models, and trust values are a private property constructed by all agents. In this way, it is not possible to talk about the reputation of agent *A*, but about the reputation of agent *A* according to the opinions of agent *B* [Sabater and Sierra 2005]. As MASs are in nature decentralized systems, this is the natural way to represent it, since most trust and reputation models for MASs are subjective. On the other hand, global visibility is available to all agents in the system and is often used by online and centralized models. One example is eBay [eBay 2015], where reputation values of each member can be observed by all the other users. Models that use only certified reputation as their information source such as Huynh et al. [2006] and Botelho et al. [2009] are classified as global because the values are centered in the agent database itself. FIRE [Huynh et al. 2004] uses certified reputation in addition to other distributed information sources, which characterizes it as a hybrid model with respect to visibility.

The second characteristic is *granularity* and it is classified as non-context dependent and context dependent. Models belonging to the first category do not make use of environmental information or specific variables of certain applications. They are multicontext, and the same model can be applied in different applications [Sabater and Sierra 2005]. Some examples are PRrep [Haghpanah and desJardins 2012] and Vogiatzis et al. [2010]. On the other hand, context-dependent models are (1) associated with specific applications where trust values need a specific context for their calculations or (2) applied only to a certain domain. Some examples are FOCET [Mokhtari et al. 2011], which uses ontologies for representation and recognition of contexts; Liu and Datta [2012], which use HMM (Hidhen Markov Model) to get information from contexts; and IRTM [Rettinger et al. 2007], which introduces the trust transfer concept among contexts. Other examples are the models by Burnett et al. [2013], Wang et al. [2008], Rettinger et al. [2008], and Bertocco and Ferrari [2008].

The third characteristic is whether the models have mechanisms to measure the *reliability* of trust and reputation calculated values. It is related to the relevance of the value in the final decision of whether to interact with the target agent. This is usually associated with the number of interactions, the reliability of testimony, or the age of the data used in the calculations [Sabater and Sierra 2005]. Some examples are the models by Carter et al. [2002], which implements weight calculations; RRFAF [Rosaci 2012], which uses reliability matrices; and SecuredTrust [Das and Islam 2012], which presents a decay model where trust values decrease over time.

The last characteristic is the *trust model,* and the review by Sabater and Sierra [2005] aims to identify if the model is related to trust or reputation. According to them, models using direct interaction are classified as trust models, while models that use witness information are classified as reputation models. However, Pinyol and Sabater [2013] argue that there is no clear consensus in the literature about the differences between these definitions, and they propose using only the trust dimension. They follow the same definitions given by Castelfranchi and Falcone [1998], that trust is considered a practical reasoning related to the final decision of whether to interact with another agent. Some models only present ways to calculate trust values, while others specify how the final decision will be made related to a decision-making process. The latter are considered trust models by Pinyol and Sabater [2013]. One example is the work by Rehák et al. [2005], which uses fuzzy logic to represent the agent's mental states in decision-making processes.

3.13. Discussions About Trust Dimensions

This section is part of our first contribution, and Table III shows all analyzed models in this review with their dimensions filled in according to the dimensions defined in Table II (the columns can be parsed using Table II). This table was constructed based on the tables defined in the reviews by Sabater and Sierra [2005] and Pinyol and Sabater [2013], and it aims to provide a wide view of the models and their dimensions. It can be used to check the literature if it is necessary to consult a trust and reputation model that presents some of the dimensions, and it is also useful to compare and evaluate models.

To fulfill Table III, we followed the same arguments discussed by Sabater and Sierra [2005], who argue that the dimensions evaluated do not always fit exactly into the models because of their diversity. In some situations, the evaluations of some models were subjective and performed according to our interpretation. Additionally, we considered only what is implicit in the papers and did not consider extensions or assumptions.

We can observe in Table III that the information sources related to the models are separated by a comma or a plus sign (third column). There is a subtle but important distinction between them. When a model presents the *DI+WI* characteristic, we mean that a calculation exists to combine both information sources, and agents' confidence is given by this combination. On the other hand, when a model presents the *DI, WI* characteristic, we mean that the two information sources are not combined. This occurs when one of the sources is not available and agents need to use the other. It is also important to clarify that according to Table II presented in Section 2, when the "$\surd$" symbol is used, we mean the model presents the dimension. Otherwise, the "-" symbol indicates that the model does not make use of it, while "NA" is set when the analyzed dimension is not applicable to the model.

Based on Table III, we constructed Table IV, which presents all the trust dimensions found in all analyzed models, indicating how many of them employ such dimensions. The objective of this table is to provide a wide view of the field, showing the most-used dimensions and the ones the community has not given so much attention to. Based on this, we can reflect on some aspects.

The first reflection is about the great interest in the development of trust and reputation models for MASs, and this can be demonstrated by the increasing number of models proposed in recent years. We argue that it is happening because MAS applications require such security mechanisms (soft security) to ensure the integrity and longevity of the system, and only hard security techniques are not suitable. Another reason is related to the global growth of e-commerce for consumer to consumer (C2C), which requires mechanisms to reduce risk in interactions among unknown members.

As addressed in the review by Pinyol and Sabater [2013] and confirmed by this article, although mathematical models have the largest amount of related work (85%), we can observe an increase in the number of cognitive and hybrid models (16%). A plausible

Table III. All Analyzed Models and Their Dimensions

	Par	InS	Che	Smn	Prf	Dlg	Rsk	Fdb	Int	Ope	Hrs
Marsh [1994]	N	DI	0	-	-	-	√	NA	-	-	-
Abdul-Rahman and Hailes [2000]	N	DI+WI	2	√	-	-	-	-	-	√	-
Schillo et al. [2000]	N	DI+DO+WI	2	-	-	-	-	√	-	√	-
Castelfranchi and Falcone [2001]	C	-	0	-	-	√	√	NA	-	-	-
Borrell et al. [2001]	N	DI+WI	-	-	-	-	-	-	-	-	√
Sabater and Sierra [2002] (Regret)	N	DI+WI+SI+P	2	√	-	-	-	-	√	-	-
Montaner et al. [2002]	N	WI	0	-	√	-	-	-	√	-	-
Mui et al. [2002]	N	DI+WI	0	-	-	-	-	-	-	-	-
Carter et al. [2002]	N	RL+WI	0	-	-	-	-	√	-	-	-
Carbo et al. [2002] (AFRAS)	C	DI+WI	0	√	-	-	-	-	-	√	-
Padovan et al. [2001]	N	DI+WI	0	-	-	-	-	-	-	√	-
Sen and Sajja [2002]	N	DI+WI	2	-	-	-	-	-	-	√	-
Josang and Ismail [2002] (BRS)	N	DI+WI	0	-	-	-	-	-	-	-	-
Jurca and Faltings [2003]	N	DI+WI	2	-	-	-	-	√	-	-	√
Carter and Ghorbani [2003]	C	DO	0	√	-	√	-	NA	-	-	-
Yu and Singh [2003]	N	DI+WI	2	-	-	-	-	-	-	√	-
Castelfranchi et al. [2003]	C	DI+WI+DO	0	-	-	-	-	-	-	-	-
Griffiths and Luck [2003]	N	DI+WI	0	-	-	-	-	-	-	-	-
Derbas et al. [2004] (TRUMMAR)	N	DI+WI+SI	0	-	-	-	-	-	√	-	-
Huynh et al. [2004] (FIRE)	N	DI+WI+CR+RL	0	-	-	-	-	-	-	√	-
Ramchurn et al. [2004a]	N	DI+WI+P	0	-	-	-	√	-	-	-	-
Song et al. [2004]	N	WI	0	-	-	-	-	-	-	-	-
Biyela [2004]	N	DI	0	-	-	-	-	NA	-	-	√
Neville and Pitt [2004]	C	DI+WI	0	-	-	√	-	-	-	-	-
Tran and Cohen [2004]	N	DI+WI	2	-	-	-	-	-	√	√	-

(Continued)

Table III. Continued

	Par	InS	Che	Smn	Prf	Dlg	Rsk	Fdb	Int	Ope	Hrs
Sierra and Debenham [2005]	N	DO	0	-	-	-	-	NA	-	-	-
Rehák et al. [2005]	N	DO	2	-	-	-	√	NA	-	-	-
Muller and Vercounter [2005] (LIAR)	N	DI+WI+SI	2	-	-	-	-	-	√	√	-
Griffiths [2005] (MDT)	N	DI	0	√	√	√	-	NA	-	-	-
Ashri [2005]	N	DI+WI+SI	0	-	-	-	-	-	-	-	-
Shi et al. [2005]	N	DI+WI	2	-	-	-	-	-	√	-	-
Wang and Zhang [2005]	N	DI+WI	0	√	-	-	-	√	-	-	-
Zheng et al. [2006]	N	DI+WI	1	-	-	-	-	-	-	√	-
Huynh et al. [2006]	N	CR	2	-	-	-	-	NA	-	√	√
Teacy et al. [2006] (TRAVOS)	N	DI+WI	2	-	-	-	-	-	-	√	-
Sabater et al. [2006] (Repage)	N+C	DI+WI	2	-	-	-	-	-	-	-	-
Regan et al. [2006]	N	DI+WI	2	-	-	-	-	-	√	√	-
Zhang et al. [2007]	C	DI+WI	2	-	-	-	-	-	-	-	-
Bentahar et al. [2007]	N+C	DI+WI	0	-	-	-	-	-	-	-	-
Li et al. [2007]	N	DI+WI+SI	0	-	-	-	-	-	-	-	-
Mokhtar et al. [2007]	-	-	0	-	-	-	-	NA	-	-	-
Nkosi et al. [2007]	N	DI+WI+RL	0	-	-	-	-	-	-	-	√
Rettinger et al. [2007] (IRTM)	-	-	0	√	-	-	-	-	√	√	-
Ghanea-Hercock [2007]	N	DI	0	-	-	-	-	NA	-	-	-
Bedi et al. [2007]	N	WI, SI	0	√	-	-	-	-	-	-	-
Dondio and Barrett [2007]	N	-	NA	√	-	-	-	NA	-	-	-
You [2007]	N	DI+WI	2	-	-	-	-	-	-	√	-
Reece et al. [2007]	N	DI+WI	0	-	-	-	-	-	-	-	-
Wang et al. [2008]	N	DI+WI	2	-	√	-	√	-	-	√	-
Yu et al. [2008]	N	DI+WI	0	-	-	-	-	-	√	-	-
Bertocco and Ferrari [2008]	N	WI	0	√	-	-	-	-	-	-	√
Li et al. [2008]	N	DI+WI	0	-	-	-	-	-	-	-	-
Gutowska and Buckley [2008]	N	DI+WI	0	-	-	-	-	-	-	-	-

(Continued)

Table III. Continued

	Par	InS	Che	Smn	Prf	Dlg	Rsk	Fdb	Int	Ope	Hrs
Hussain et al. [2008]	N	DI+WI	0	-	-	-	-	-	-	-	-
Pinto [2008]	C	DI+WI	0	-	-	-	-	-	-	-	-
Teacy et al. [2008]	N	DO	0	-	-	-	-	NA	-	√	-
Reches et al. [2008] (IASU)	N	DI+WI	0	-	-	-	-	-	-	-	-
Rettinger et al. [2008] (IHRTM)	N	DO	0	-	-	-	-	NA	√	√	-
Keung and Griffiths [2008]	N	DI+WI	0	√	-	-	-	-	-	√	-
Khosravifar et al. [2009]	N	DI+WI	0	-	-	-	-	-	-	-	-
Botelho et al. [2009]	N	CR	0	√	-	-	-	NA	-	√	√
Tian et al. [2009] (RMNRS)	N	DI+WI	0	-	-	-	-	-	-	-	-
Tong et al. [2009]	N	DI+WI	2	-	-	-	-	-	-	-	-
Lei et al. [2009]	N	WI	0	-	-	-	-	-	-	-	-
Zhou et al. [2009] (CORE)	N	WI	0	-	-	-	-	-	-	-	-
Urzica [2010]	N	DI+WI+RL	0	-	-	-	-	-	-	-	-
Elgohary et al. [2010]	N	WI	0	√	-	-	-	-	-	-	-
Klejnowski et al. [2010]	N	DO+SI	0	-	-	-	-	NA	-	-	-
Vogiatzis et al. [2010]	N	DI+WI	0	-	-	-	-	-	-	-	-
Hermoso et al. [2010]	N	RL	0	-	-	-	-	NA	√	√	-
Matt et al. [2010]	N+C	DI	0	√	-	-	-	NA	-	-	-
Aboulwafa and Bahgat [2010] (DiReCT)	N	DI+WI	2	-	√	-	-	-	-	-	√
Yaich et al. [2011] (ASC-TMS)	N	RL	0	-	-	-	-	NA	-	√	-
Parsons et al. [2011]	N+C	WI	0	-	-	-	-	-	-	-	-
Erriquez et al. [2011]	N	-	0	-	-	-	-	NA	-	-	-
Burnett et al. [2011]	N	-	0	-	-	√	√	NA	-	√	-
Mokhtari et al. [2011] (FOCET)	N	DI+WI+P+RL	0	-	√	-	-	-	-	√	-
Urzica et al. [2011]	N	DI+WI	0	-	-	-	-	-	-	√	-
Liu et al. [2011] (iCLUB)	N	WI	2	-	-	-	-	-	-	-	-
Liu and Datta [2011]	N	DI+WI	0	√	-	-	-	-	-	√	-

(Continued)

Table III. Continued

	Par	InS	Che	Smn	Prf	Dlg	Rsk	Fdb	Int	Ope	Hrs
Singh [2011]	C	DI	0	-	-	-	-	NA	-	-	-
Venanzi et al. [2011]	C	DO	0	-	-	√	√	NA	-	-	-
Koster et al. [2011]	N+C	WI	0	-	√	-	-	-	-	-	-
Chopra et al. [2011]	C	RL	0	-	-	√	-	-	-	-	-
Rosaci [2012] (RRAF)	N	DI+WI	0	-	-	-	-	-	-	-	-
Teacy et al. [2012]	N	DI+WI+DO	0	-	-	-	-	-	-	√	-
Pinyol et al. [2012] (BDI + Repage)	C	DI+WI	0	-	-	-	-	-	-	-	-
Das and Islam [2012] (SecuredTrust)	N	DI+WI	2	-	-	-	-	-	-	-	-
Khosravifar et al. [2012] (CRM)	N	DI+WI	2	-	√	-	-	-	-	√	-
Sharma et al. [2012]	N	DI+WI	2	-	-	-	-	-	√	-	-
Serrano et al. [2012]	N	DI+WI+DO	0	-	-	-	-	-	-	-	-
Klabi et al. [2012]	N	DI+WI	0	√	-	-	-	-	-	-	-
Sutcliffe and Wang [2012]	C	SI	0	-	-	-	-	NA	-	√	-
Rosaci et al. [2012] (TRR)	N	DI+WI	0	-	-	-	-	-	-	-	-
Haghpanah and desJardins [2012] (Prep)	N	DI,WI	1	-	-	-	-	-	-	-	-
Fang et al. [2012] (Sarc)	N	DI+WI	2	-	-	-	-	-	-	√	-
Salehi-Abari and White [2012] (DART)	N	DI+WI+DO	2	-	-	-	-	-	-	√	-
Liu and Datta [2012]	N	WI	2	-	-	-	-	-	√	-	-
Piunti et al. [2012]	C	DO	0	-	-	√	-	-	-	√	-
Liu et al. [2012]	N	DI+WI+P+SI	0	√	-	-	-	-	-	√	-
Burnett et al. [2013]	N	DI+WI+P	2	-	-	√	-	-	√	√	-
Su et al. [2013] (Priority-Based)	N	DI+WI	2	√	√	-	-	-	-	√	-
Wang and Gui [2013]	N	DI+WI	2	-	-	-	-	-	-	-	-
Liu et al. [2013b]	N	DI+WI	0	√	-	-	-	-	-	√	-
Fang et al. [2013] (DiffTrust)	N	DI+SI+DO	0	-	-	-	-	-	√	√	-
Liu et al. [2013a]	N	WI	2	-	-	-	-	-	-	-	-

Table IV. Trust Dimensions

Paradigm type		Information sources					
C	N	DI	WI	SI	CR	P	RL
18/106 (16%)	91/106 (85%)	73/106 (68%)	79/106 (74%)	10/106 (9%)	3/106 (2%)	5/106 (4%)	8/106 (7%)
Cheating assumptions			Trust semantics	Trust preferences	Delegation	Risk measure	Incentive feedback
L0	L1	L2					
72/106 (67%)	2/106 (1%)	30/106 (28%)	19/106 (17%)	8/106 (7%)	9/106 (8%)	7/106 (6%)	4/106 (3%)
Initial trust			Open environment			Hard security	
15/106 (14%)			37/106 (34%)			8/106 (7%)	

explanation is the growth of the interest in applications that consider the cognitive aspects closest to human behavior, instead of only simple scenarios. An example is the argumentation process, which requires more reasoning and complex agents, different from purely numeric ones (Section 4.2). Despite this, most models are interested only in providing resources for simple cooperation or partner selection, and they do not take into account these aspects. We think this scenario will change in a few years and researches will focus their work on the cognitive and affective aspects of trust. Regarding affective aspects, Johnson-George and Swap [1982] and McAllister [1995] define affective trust as a kind of trust related to strong emotional content given by the level of care and concern the partner shows, based on the emotional bonds developed between individuals.

With respect to information sources, we can observe in Table IV that most models employ direct interaction (68%) and witness information (74%). We have the same conclusions from the review by Sabater and Sierra [2005], that this is due to the fact that direct interaction and witness information are the most common ways to extract information from other agents, and often they are used in e-commerce scenarios, which is the most-implemented application in most models. Another reason is that, as stated on Section 3.2.1, direct interaction is considered the most valuable information source. Despite this, we have seen an increasing number of models employing different information sources, such as sociological information (9%), certified reputation (2%), prejudice (4%), and rules (7%). Although these numbers are not significant compared to the amounts of the models, we can realize the growing interest in finding new ways to extract information from agents and from environments. Based on the original review by Sabater and Sierra [2005], we have found two more information sources: certified reputation and rules. Another related issue is the incentive feedback dimension, which is used by only 3% of the models. We realize this dimension is rather important when dealing with witness information, so it would be recommended that both dimensions work together.

As open MASs are designed to host large amounts of agents, it is necessary to reduce risk in interactions, since many of them may be unknown or malicious. This issue can be addressed by the cheating assumption mechanisms, and based on Table IV, 28% employ these mechanisms. Most models do not take this dimension into account (67%), and 1% deal with biased information. We think this dimension is rather important for MASs, since the probability of cheaters in open environments is high.

Another dimension we analyzed is the open environment, which is composed by 34% of the models. We can realize that many models deal with this, and we think this is due to the fact that as MASs are often open, mechanisms to guarantee the security of the environment are necessary. We also argue that the growth of open MASs is directly proportional to the growth of trust and reputation models. Another related dimension is the construction of initial trust, which is employed by 14% of the models. We argue that open environment and initial trust are related because in open environments, where agents can enter and leave at any time, it is necessary to calculate initial values to newcomers. We think that MASs must implement both dimensions.

Delegation is a dimension introduced by Castelfranchi and Falcone [1998] and is employed by 8% of the models. The authors argue that trust happens in delegation scenarios, but there are few models that use task delegation in applications and evaluations. A related dimension is risk measure, which can be applied together with delegation, since it would be plausible to estimate risks before delegating tasks. In MASs, both dimensions should be implemented together. With respect to risks, Lu et al. [2009] state in their review that just a few models employ risk measures, and they argue that it is a deficiency in the field. Based on Table IV, we have found that this scenario has not changed yet, since only 6% of the models deal with this issue.

As discussed in Section 3.4 and Section 3.5, trust semantics and trust preferences are dimensions related to each other, and 17% deal with the former and 7% with the latter. Lu et al. [2009] also state in their review that the semantic dimension is not widely used, and based on Table IV, we conclude that this scenario has changed a little, since we can observe several models dealing with it. On the other hand, there are few models using preferences, and we argue that this is complementary to semantics because some variables (semantic) must exist to define weights afterward.

The last dimension is hard security, and we can observe in Table IV that only 7% employ this kind of mechanism. Within MASs, it is important to prevent information from being modified or captured, so we argue that it is necessary to combine soft and hard security, as in the DiReCT model [Aboulwafa and Bahgat 2010]. Perhaps the basic security mechanisms addressed by some authors are a premise of infrastructure that is not explicitly declared in the trust model.

Based on Table III, we realize it is not common to find models that implement various dimensions concomitantly. It happens because each model usually focuses its contribution on a specific dimension, prioritizing all the efforts only on that dimension. However, this does not mean that models with few dimensions are worse than the ones that present a wide variability of dimensions. On the other hand, models with great variability are not better than others, since they can deal superficially with each dimension. The objective of this analysis is to show the main dimensions that exist in the literature, present how the models employ it, and show how they are applied in MASs. It is not our aim to identify the better model or critically analyze them.

Finally, an issue presented by Sabater and Sierra [2005] and reaffirmed by Pinyol and Sabater [2013] is the low quantity of tools and frameworks to help developers in the comparison of models for MASs. However, there are efforts related to this in the field, some of which are specific to certain problems such as e-commerce and most of which have low generalizability to other kinds of applications. Nowadays no frameworks exist that are capable of dealing with the most recent approaches to trust and reputation models.

4. INTERACTION-BASED MULTIAGENT DIMENSIONS

Based on interaction models addressed by Wooldridge [2009] and Ferber [1999], the purpose of this section is to define each type of interaction and describe how it can be used in trust and reputation models for MASs. This section presents our main contribution, and it is based on the three questions defined in the introduction: (1) What is the most common set of dimensions that has been used in the literature? (2) What are the relations of these dimensions with the type of interaction? (3) What are the other

Table V. Types of Interaction and Related Models

Coalition (23%)	Argumentation (13%)
Griffiths and Luck [2003]	Bentahar et al. [2007]
Rehák et al. [2005]	Matt et al. [2010]
Ghanea-Hercock [2007]	Parsons et al. [2011]
Tong et al. [2009] (LCCM)	Koster et al. [2013]
Lei et al. [2009]	
Zhou et al. [2009] (CORE)	
Erriquez et al. [2011]	
Negotiation (51%)	**Recommendation (13%)**
Schillo et al. [2000]	Montaner et al. [2002]
Ramchurn et al. [2004a]	Song et al. [2004]
Tran and Cohen [2004]	Bedi et al. [2007]
Sierra and Debenham [2005]	Hermoso et al. [2010]
Regan et al. [2006]	
Rettinger et al. [2007] (IRTM)	
You [2007]	
Rettinger et al. [2008] (IHRTM)	
Teacy et al. [2008]	
Tong et al. [2009] (LCCM)	
Urzica et al. [2011]	
Yaich et al. [2011] (ASC-TMS)	
Rosaci [2012] (RRAF)	
Klabi et al. [2012]	
Rosaci et al. [2012] (TRR)	
Liu et al. [2013a]	

important dimensions not covered by the literature? As stated before, the answers to these questions may assist developers in choosing the set of dimensions to be used according to the types of interaction.

Table V lists the types of interaction considered in our work with their related models. They were selected by analyzing each one of the models and checking what kind of interaction was applied in MASs. It is important to emphasize that the models listed in Table V are the same we analyzed previously, and we only looked for characteristics of MASs in each one of them. Although there is a broad range of types of interaction found in MAS, we have discussed only the ones presented in the analyzed models. We have studied the total amount of 106 models, and among them only 31 (29%) present specifics characteristics related to coalition, argumentation, negotiation, and recommendation. From these 31 models, we can see from Table V that 23% are related to coalition, 13% to argumentation, 13% to recommendation, and most of them to negotiation (51%). We understand this is the case because most of the applications and models are developed for e-commerce scenarios. Despite this, we can realize an increasing number of models related to other types of interaction on MASs.

Cooperation and partner selection interactions were not considered because they are implicitly present in all trust and reputation models. For example, an agent is cooperating in the system when he or she reports correct information to others or behaves correctly (cooperation). On the other hand, the basic purpose of trust and reputation mechanisms is to assist agents in choosing the best partners to interact with (partner selection). We see that 71% of all analyzed models fit these characteristics.

The following sections present each one of the types of interaction and explain how the models employ trust and reputation concepts according to coalition, argumentation, negotiation, and recommendation. Within each section, a discussion about the three questions is given.

4.1. Coalition

Coalition is a type of cooperation where agents are grouped to solve complex problems that alone they would not be capable of solving. Another objective of coalition is increasing the usefulness of the group. The team's formation through coalition is typically performed based on agents' abilities according to each task. The tasks are usually decomposed into subtasks, so agents can solve them using their specific skills [Wooldridge 2009; Ferber 1999]. It is also an important method used to solve complex tasks where a maximum payoff should be obtained by the individuals and by the whole group. Generally, it is short term and oriented to specific objectives, being dissolved when it is completed. As stated before, coalition is a type of cooperation; therefore, there are two ways to cooperate in coalitions. The first is when an agent has specific skills to complete a given task and is invited to join a coalition. In this context, this agent deciding to join the group is a sign of cooperation; otherwise, it is assumed that the agent is defecting. The second case occurs when an agent is already working in a coalition, so if this agent is fulfilling his or her tasks, it is a signal of cooperation; otherwise, it is assumed that the agent is not cooperating with the whole group. Both kinds of cooperation are addressed by some models, which are described later.

The model by Rehák et al. [2005] uses fuzzy numbers to represent trust and deals with uncertainty. Agents within a community learn to identify defector members and progressively refuse to cooperate with them. This is done by a method that permits agents to access the reliability of each partner of the coalition, using a utility function that returns the results of cooperation inside the coalition. Each member receives a single value of 0 or 1, which represents the observations of other members of the coalition, given by a function that calculates the minimum and maximum utility. Another feature presented in this model is the concept of self-trust as a parameter for decision making. As an example, we can talk about the scenario in which an agent needs to protect the environment and some malicious software is trying to steal personal information. When this agent realizes that his or her confidence in protecting the environment is decreasing, he or she can migrate to another environment or stop the communications with others to protect the whole coalition. The last important feature discussed in this model is the process of making a decision about cooperating or defecting. When an agent organizes a coalition, he or she identifies a set of trusted agents and calculates the utility of them using their social acquaintance presented in the social knowledge model. The utility of the agents is multiplied by their confidence, which measures their willingness to enter the coalition. On the other hand, the opposite happens when the agent is invited to join a coalition.

Similarly, in the LCCM model [Tong et al. 2009], agents decide to join a coalition based on utility and trust. The trust-building process is based on direct interactions among agents and is related to the confidence of each member. The coalition's reputation is based on direct observations and is reflected by the numbers of agents participating minus the number of agents leaving the group. If an agent observes that others have entered the coalition, it means that reputation is increasing and it has a greater weight. Before joining a coalition, agents will first check its reputation, preferring the most-populated and trustful groups, which decreases their likelihood of being exploited.

Another model about coalition is the one developed by Griffiths and Luck [2003], which addresses coalition formation using motivation and trust. Motivation allows representation and reasoning about goals, while confidence presents mechanisms for reasoning about trust, honesty, and veracity. The authors discuss the concept of clans, which are formed by groups of agents who trust each other and have similar objectives. The utility of a group is measured according to the proportion of contributions of each agent to achieve the goals. On the other hand, (1) motivations determine if agents

Table VI. Dimensions of Coalition Models

Paradigm Type	Information Sources				
N	DI	DO	WI	Risk Measure	Cheating Assumptions
7/7 (100%)	2/7 (28%)	1/7 (15%)	4/7 (57%)	1/7 (15%)	2/7 (28%)

want to cooperate, (2) intentions determine if they have the abilities to cooperate, and (3) trust determines the perceived risks in cooperating. This model also addresses the communication costs among agents, in the sense that once a plan is formed, it is necessary to estimate the trust and motivation of each agent within the environment to form the best group.

CORE [Zhou et al. 2009] focuses on task execution within the coalition and takes into account the aspects of competence and reputation. A Euclidian distance calculation is made to measure competence and verify similarity, while reputation is given by a membership function. To form a new coalition, the appropriate agents are selected according to their trust value, and after the task is started within the coalition, agents are evaluated according to their competence in fulfilling the tasks. In this way, the reputation of agents is updated and this measure is used later in delegating new tasks.

The work by Ghanea-Hercock [2007] considers the requirements for stable high-trust coalitions to self-organize and survive, even if there are malicious agents in the environment. Agents use direct interaction to update their internal confidence in other members and use these values to change their likelihood of cooperation or defection based on the expected behavior of most of their neighbors. As an example: if most of the neighbors defect, the probability that a particular agent has the same behavior increases. On the other hand, if agents experience a sequence of cooperative interactions, they tend to form high-trust groups. In other words, this model aims to increase the resilience and resistance to defection.

Erriquez et al. [2011] use the concept of distrust to form a coalition. They argue that most studies use trust and reputation only to rank agents according to their confidence level, aiming to choose the better afterward. According to these authors, these models lack a global view because they consider the agents only before forming the coalition and not when it is already formed. To address this issue, they propose a model that computes trust after the tasks in the coalition are already happening. They consider a coalition free of suspicion if any member distrusts the others, arguing that this is the basic requirement to a trustful coalition.

Finally, the work by Lei et al. [2009] focuses on coalition formation applied in migrating workflow in business processes, and they use direct experiences and witness information to extract trust information and compute trust values. No more details are given about this model because its main focus is about workflow.

CORE [Zhou et al. 2009] and LCCM [Tong et al. 2009] address the stability problems that often happen in coalitions, where an agent can leave the coalition and form a new one. This issue may represent a problem because when an agent leaves the group, it might be difficult to find another one with the same skills for replacement. In this context, trust and reputation mechanisms may help to solve this problem.

Table VI presents all the trust dimensions found in these models, indicating how many of them employ such dimensions. According to our second contribution, the objective of this table is to find a link between trust dimensions and types of interaction in MASs so we can observe which dimensions are present. This table also provides the answer to the first question, since it is possible to see the most common dimensions used in the literature according to this type of interaction.

To answer question two, we can observe from Table VI that all models employ the numeric paradigm. This happens because all of them use only aggregation of numbers, and no cognitive mechanisms are employed. As these works usually use utility functions or the quantity of members to compute trust, we argue that no mechanism similar to human behaviors was necessary for this type of interaction, so the numeric paradigm is suitable. Additionally, the use of mathematical models simplifies the development of algorithms for partner selection, since complex cognitive procedures for information retrieval are not necessary.

With respect to the information sources, we can see that witness information is the most used, and this is plausible since in an MAS the agents have not always interacted with others and they need information about them. Another issue is that when the tasks are short term, coalition formation must occur very quickly without wasting time in complex ranking processes. For these reasons, the use of witness information is a viable alternative that allows reputation calculation without direct interactions, which would delay the information retrieval process. An interesting aspect is that direct observation is used only by Rehàk et al. [2005], and we argue that this information source can be very useful to form a coalition, since it is possible to observe the agent's behavior when he or she is participating in a coalition.

Cheating assumptions are employed by just two models, and it is an important dimension to take into account in an already-formed coalition, as the agents participating in the group may cheat and affect the whole utility of the group.

Only the model by Rehàk et al. [2005] employs the risk measure, which is a very important parameter to use when deciding about inviting a new member into a coalition. Lu et al. [2009] address this issue in their review, showing that few models deal with risk measures, so it is a dimension not much explored in the field.

Finally, we answer question three by noting that none of the models focuses on task delegation, which is a natural scenario in coalitions. MASs based on coalition usually need to solve complex tasks, which are divided into more or less complex tasks and delegated to agents according to their skills. For this reason, beyond the dimensions shown in Table VI, we additionally recommend the use of the delegation dimension.

4.2. Argumentation

An argumentation system integrates several different arguments to reach a final conclusion in a particular subject, and it usually consists of a pair of arguments and attacks on these arguments, in order to consider just the acceptable ones. These arguments are stored in a knowledge base often used in dialogues between agents. It is a reasoning process, and some studies have already used this method for reasoning about interacting or not interacting in a trust environment. It is well suitable for MASs and robust against inconsistencies, uncertainty, and knowledge contradiction, which can be applied in communication among agents. Unlike classical communication protocols used in MASs such as FIPA ACL (Agent Communication Language), argumentation-based dialogue protocols are flexible and better suited to agents equipped with reasoning mechanisms. Argumentation can be used to reason about what kind of information to consider in a decision-making process, and different arguments among agents can lead to conflicts. In multiagent systems, the revision of beliefs and decisions generates conflicts, since agents can have different points of view about a subject. In this context, a set of arguments is free from conflict if there is no argument attacking it [Amgoud and Cayrol 2002]. For these reasons, trust and reputation techniques are useful in this kind of system to guarantee the confidence of arguments.

The model proposed by Parsons et al. [2011] evaluates the combination of a formal trust model with a formal argumentation model. It uses a trust graph to represent confidence constructed by direct and indirect experiences, where agents are the vertices and edges are represented by the trust level. On the other hand, the argumentation system is used to reason about agents' beliefs through an equation that computes the

Table VII. Dimensions of Argumentation Models

Paradigm Type	Information Sources			
N+C	DI	WI	Trust Semantics	Trust Preferences
4/4 (100%)	2/4 (50%)	3/4 (75%)	1/4 (25%)	1/4 (25%)

level of belief in a specific argument. If an agent provides information that he or she does not trust very highly, the agent will not derive conclusions from this information. In other words, information acquired from unreliable sources is not sufficient to defeat arguments made from more reliable ones, so the beliefs are affected by trust values.

Matt et al. [2010] address vulnerability of agents in scenarios where they can violate contracts, and the proposed model aims to reduce this problem by combining statistics and arguments. Statistics indicate past interactions, while arguments are used to make future predictions about agents' behavior. They consider two types of arguments: forecast and mitigation. Forecast arguments are related to dependence on the existence or absence of contractual clauses that regulate agents' behavior, and they can be seen as justified claims related to expected or anticipated behaviors of the target agent. On the other hand, mitigation arguments attack forecast arguments and depend on the violation of the terms of the contract, being used to express uncertainty concerning the evaluator's forecast arguments. This fact may reduce the strength of arguments, since the stronger ones are considered more trustful than the others. Arguments are taken into consideration according to their strength and how much stronger they are, increasing the impact of computing trust.

In the model by Bentahar et al. [2007], agents can reason about the reputation of others using their own argumentation system. It uses dialogue game techniques to perform communication, which are interactions among agents in which each agent performs declarations according to a set of predefined rules. Agents use the reasoning and argumentation mechanisms to decide the next performative to be used, based on formal dialectics where the arguments are used to represent decision-making processes. The model uses previous experiences and reputation graphs to compute trust, and the final trust value is given by these values combined with the total amount of acceptable arguments.

The model proposed by Koster et al. [2011] extends the AdapTrust [Koster et al. 2013] argumentation framework, which is an extension of the BDI architecture. This argumentation framework allows agents to discuss and adapt their trust models. This is done when agents try to persuade others that their own beliefs about the environment in their trust models are correct and that others' beliefs are wrong. Each agent builds his or her own argumentation system based on his or her own model of trust and uses a dialogue protocol that allows two agents to compare their trust ratings in order to find out how their trust models diverge. The adaptations on trust models are done using preferences and priority rules, so if an agent believes time is more important than delivery, the argumentation system will be adapted to enable such customization.

Table VII presents the trust dimensions related to the argumentation models, and it provides the answer to the first question, since it is possible to observe the most common dimensions used in the literature according to this type of interaction.

To answer the second question, we note that all models are hybrid (cognitive and numeric). Some of them employ the numerical paradigm by using numerical aggregations of direct interaction and witness information with the quantity of valid arguments. On the other hand, the cognitive paradigm is suitable because an argumentation task may be considered a cognitive process, and argumentation is used to reason about beliefs and contracts, being close to BDI architectures. Due to the high complexity of argumentative interaction analysis done by the model, we understand that this is the best paradigm for this type of interaction. Unlike the mathematical models, cognitive models can acquire knowledge through perception and various information sources, including dealing with the complex argumentative language.

We argue that models in this category use only the most common information sources (direct interaction and witness information) because most of them calculate trust using already-existing techniques in the literature, and the argumentation framework is added to these models to aid in trust calculation. This is another explanation for all of them being hybrid.

With respect to semantics and preferences, we can observe in Table VII that only two models employ these dimensions. We argue that in an argumentation system, agents need to specify these parameters, since the creation and understanding of arguments could be easier for others. By using these dimensions, agents can specify which parameters will be used [Matt et al. 2010] and the weight of each one [Koster et al. 2013].

We can observe that the developing process of a trust and argumentation model might be rather complex, since it is necessary to build mechanisms to analyze the content of arguments exchanged between agents. Another issue is the development of a knowledge base consisting of attack and defense arguments that could be used in communication. It is also necessary to address the definition of a set of parameters about how to interact with other agents using their argumentative framework.

Finally, we answer question three by noting that although this review did not identify argumentation models based on open environments, we believe it would be viable to explore this possibility. In a cognitive environment in which knowledge may be acquired from exchange of arguments, this may represent an opportunity to deal with the heterogeneity of open MASs. We hypothesize that the more numerous and heterogeneous the community of agents is, the greater the possibility to learn during the argumentation process. Regarding information sources, we also believe the use of rules would be an important mechanism to standardize the variables of arguments, so agents could trust only in arguments that respect the rules defined in the system.

4.3. Negotiation and Competition

There are some interaction models that present competition situations among agents, which usually happen when conflicts of interests exist that are often motivated by resource scarcity, the struggle for existence, or conflicting goals. In environments consisting of competitive agents, agents can show fraudulent behavior by creating problems for their competitors and increasing their own utility. In this context, trust mechanisms are important to choose just the reliable agents to interact and compete with. Negotiation is a competition interaction type useful for building agreements for conflict resolution, and the most-explored field in MASs is e-commerce. The continuous growth of the e-market is a factor that motivates research in the design of trust models that allow a secure environment in negotiation, representing alternatives to reduce risks in interactive open societies.

AVALANCHE [Padovan et al. 2001] is a prototype for an agent-based secure electronic commerce marketplace environment. This project provides security strategies to eliminate fraudulent agents, addressing three common problems for any open electronic marketplace environment: (1) authentication, (2) privacy of communications, and (3) lack of cooperation for sharing information. In the simulations presented by the authors, each agent can choose a type of strategy: greed, price change, prenegotiation, satisfaction, memory, or reputation. With the use of these strategies, it is possible to determinate agents' cooperative behavior.

Tran and Cohen [2004] propose a framework for modeling an electronic marketplace where buyers and sellers can evaluate their interactions, allowing the construction of a reputation model based on user satisfaction. Another contribution of this paper is the proposition of reinforced learning algorithms for buyers and sellers. Regan et al. [2006] introduced BLADE, a trust model for buying agents in the e-marketplace, which is strongly oriented on the subjectivity interpretation of reviews of witness information. The seller's reputation in BLADE is continuously adjusted according to the outcome of each transaction, and aspects such as subjectivity evaluation through Bayesian networks are addressed. Another strategy to reduce risks by detecting rogue sellers is proposed by Urzica et al. [2011] using the *Liar Identification for Agent Reputation* method, which is a negotiation framework where reputation represents the guarantee of fulfillment of agreements among agents. This model defines two types of agents: the standards and the central authority. The former represents buyers and sellers in the environment, while the latter is a central agent that obtains and shares information and about the reputation of all agents in the e-marketplace.

The work conducted by You [2007] introduces trust negotiation relevance in e-commerce systems. The author defines agents' reputations based on aspects such as interaction time, price of traded goods, and volume of transaction. Another characteristic is the combination of direct interaction with reputation information using different weights, and this is done incrementally at the time the transactions occur in the e-marketplace. Fang et al. [2012] propose a model where a subjectivity alignment approach for reputation computation (SARC) is used, and the main contribution is that it deals with the subjectivity of different agents' profiles. The subjectivity of buyers is obtained by learning algorithms that analyze evaluations of other agents in the environment. It is used in Bayesian learning for internal attributes and regression analysis of external attributes.

The model by Klabi et al. [2012] integrates trust concepts in a combinatorial auction. The model uses differences between beliefs to permit checking the accuracy of data received from other agents. As an example, if agent *A* proposes $300 for a service and agent *B* believes that the fair value is $100, *A* can conclude that *B* is dishonest. In short, if there is a large difference between agents' beliefs, the target of evaluation is not considered reliable.

On the other hand, the model by Sierra and Debenham [2005] presents a rich decision model for negotiation among agents involving multiple issues, taking into account aspects of preferences and trust. It is based on information theories and focused on dialogue management between agents so that they can make informed decisions. It is performed through the observation of environmental variables and conversations between agents using a negotiation language. IRTM [Rettinger et al. 2007], in turn, can make predictions about agents' negotiation strategies, so it can automatically adjust the trading strategy based on environmental changes. Another contribution of this work is the application of initial trust techniques in open environments where agents are not known. To evaluate the experiments, the authors proposed a trading framework for MASs.

Other models that present negotiation applications are IHRTM [Rettinger et al. 2008] and Ramchurn et al. [2004a], which show trading scenarios using data from eBay [eBay 2015] and the use of contracts between agents. IHRTM [Rettinger et al. 2008] aims to group entities into classes using machine-learning algorithms, such as decision trees and support vector machines. On the other hand, Ramchurn et al. [2004a] use contracts as an agreement between agents in a negotiation process, where fuzzy numbers are used to determine if agents are able to successfully fulfill their contracts.

A number of works have used competition scenarios as a benchmark to evaluate trust and reputation scenarios. The models are not specific for competition, and they can be applied in other scenarios and some other types of interactions. Some examples are the models RRAF [Rosaci 2012] and TRR [Rosaci et al. 2012], which define criteria

Table VIII. Dimensions of Negotiation Models

Paradigm Type	Information Sources				Incentive Feedback	Open Environment	Cheating Assumptions	Risk Measure	Trust Semantics
N	DI	DO	WI	RL					
16/16 (100%)	10/16 (62%)	4/16 (25%)	11/16 (68%)	1/16 (6%)	1/16 (6%)	9/16 (56%)	6/16 (37%)	1/16 (6%)	2/16 (12%)

for weight choice associated with trust and reputation values, used as a competitive strategy. These models were tested under a scenario where agents are evaluators of paintings and they ask or give opinions to other agents, where the possibility that they are lying exists. Agents receive money for each evaluation, and the winner is the one with the largest amount of money at the end of the game.

The model by Teacy et al. [2008] uses an e-commerce scenario composed by service providers that compete for information about their competitors, and each provider needs to pay a certain amount of money to obtain this information. Within this competitive environment, agents must evaluate and decide how much they are willing to pay for information. On the other hand, they also have to be aware about the risks of receiving false information, which may reduce their utility. ASC-TMS [Yaich et al. 2011] presents its evaluations in a virtual organization environment focused on innovation communities. These communities are inherently competitive because there are several competing groups trying to solve the same problem at the same time. Other examples of models applied in competitive scenarios are LCCM [Tong et al. 2009] and Liu et al. [2013a].

Table VIII presents the trust dimensions related to the negotiation models, and it provides the answer to the first question, since it is possible to check the most common dimensions used in the literature according to this type of interaction.

To answer the second question, we can observe in Table VIII that all models are numeric, and we argue that this is because most of them are applied to e-commerce scenarios, such as applications similar to eBay [eBay 2015]. In this kind of application, direct interaction and witness information are used to compute trust, and as we can see in Table VIII, most models employ these information sources. For these reasons, we think there are no cognitive approaches of trust for competitive applications, since trust calculations depend on aggregations rather than reasoning mechanisms.

Some other models use direct observation to externally observe the behavior of sellers, and only one model employs rules to predefine the parameters of the products. We realize that a variety of information sources were used in this type of interaction, since many sources could be consulted in negotiation scenarios.

With respect to open environment and cheating assumptions, many models deal with these issues, since most e-commerce applications occur in open environments where the probability of there being cheaters is high. In this context, it is necessary to develop mechanisms to protect the honest agents. As many models implement witness information, it should be interesting to employ the incentive feedback dimension, since agents would have motivation to provide more reliable information. We can see that only Schillo et al. [2000] takes this dimension into account.

Another interesting dimension implemented by just two models is trust semantics. In e-commerce scenarios, buyers will often specify the most important parameters according to their needs, such as price, quality, or delivery. Based on these, they will select an appropriate seller according to reputation values related to one of these parameters. Additionally, risk measure is employed only by Ramchurn et al. [2004a].

Finally, we finish this section discussing question three by addressing the paradigm type. Based on the pure negotiation models analyzed, we think it is necessary to understand the communication context among agents, aiming to evaluate not only the outcome of contracts but also the messages exchanged between them. This would provide an opportunity to implement a cognitive or even a hybrid model that considers reasoning and cognitive aspects of negotiation. Nowadays, most e-commerce systems store the textual feedback from their members; however, the reputation models consider only numerical information and the human users have to perform the cognitive evaluation themselves based on the textual reviews written. We understand that the evolution of cognitive models can help in the design of reputation models that are more efficient than the purely mathematical ones, where the model, instead of human users, would do the cognitive reasoning.

We also argue that other information sources can contribute to negotiation models, such as prejudice in interacting with new sellers and sociological information to analyze the seller's or buyer's interaction network. Interestingly, we have found only one model that employs rules to predefine the behavior of agents in the environment. We think this is a very important information source to be applied in this type of interaction, since the behaviors of buyers and sellers would be standardized and no one could act differently from the predefined norms in the system. It is particularly relevant to negotiation scenarios, where sellers would not sell poor-quality products, for example. Another related issue already discussed in previous sections is that the trust preference dimension is related to semantics, but no model employs both of them together.

The last dimension we think is rather important in this type of interaction is hard security, which can promote the growth of the use of models in open negotiation environments, since they require rules and security policies to reduce the chances of fraud.

4.4. Recommendation

A multiagent recommender system aims to select products or services based on user interests, such as books, films, travel agencies, and flight companies, among others. MAS applications have given attention to this kind of system, in which agents are responsible for fetching the data, filtering it, and returning useful information to users. This process is done by querying other agents, who will recommend or not recommend certain items. When applied to MASs, a recommender system becomes a distributed world composed by recommender agents, who can be considered as personal entities that can be trustworthy or not. Recommender agents ask their trusted friends for an opinion related to an item and filter large amounts of data. In this scenario, trust is denoted by a value indicating the evaluation that agents gave to their neighbors. In traditional recommender systems, when users receive the wrong opinions, the system often has no way to ignore them, causing loss of performance in recommendations. In this context, the use of trust and reputation models is justified, since only reliable opinions are considered. This section differs from Section 3.2.3 (witness information) in the sense that there, the objective was to show and summarize some works that use witness as an information source, independently of applications. On the other hand, this section focuses on multiagent recommender systems, presenting how trust and reputation dimensions can be used to construct this kind of architecture. The model by Montaner et al. [2002] implements recommender agents using techniques to search for similar agents who have similar preferences, interests, and styles. Trust is given by filtered information and opinions of trusted agents who are in the recommender's contact list. According to the similarities between others' opinions and their own opinions, agents are able to infer a trust value for each neighbor and make recommendations afterward. The proposed approach is a hybrid and (1) is opinion based using trust

Table IX. Dimensions of Recommendation Models

Paradigm Type	Information Sources			Trust	Trust	Initial	Open
N	WI	SI	RL	Semantics	Preferences	Trust	Environment
4/4 (100%)	3/4 (75%)	1/4 (25%)	1/4 (25%)	1/4 (25%)	1/4 (25%)	2/4 (50%)	1/4 (25%)

metrics, (2) is content based, and (3) consists of collaborative filtering. The model also deals with a weight function that computes the similarity between agents according to preferences on products, keeping on the agent's list only the agents with similar interests. The authors also discuss the performance problems in recommender systems that employ trust and reputation mechanisms. These occur because it is costly to get information from all agents' in the network, so they filter information from only some parts of the environment.

The model proposed by Bedi et al. [2007] presents an application for selection of travel agencies, and it covers aspects such as destination, flight schedule, and costs. It corresponds to the semantic dimension of trust models, and the knowledge is stored in ontologies. As these dimensions are dynamic according to the environment, the authors apply temporal ontologies to absorb the environmental changes using fuzzy sets. Similar to Montaner et al. [2002], similarity between agents is used to update the trust value, and additionally, a social network is built based on trust, which agents use to generate recommendations. Each agent computes the degree of importance of the products according to their recommendation list, so the differences between opinions with others can be measured. Depending on the difference, the agent will or will not update others' trust value.

The work by Song et al. [2004] presents an approach that uses artificial neural networks to evaluate multiple recommendations, being applied in the selection of qualified recommenders. Trust is given by the number of times agents were positively qualified in recommendation processes. Additionally, recommenders who have had experience with some kind of product are indicated to create the trust net, serving as an input parameter for the construction of the training dataset for the neural network. As we can realize, this model is related to the development of an algorithm to filter opinions, and the test scenario is composed by agents who recommend movie files.

Finally, the model developed by Hermoso et al. [2010] uses rules (Section 3.2.7) to calculate trust. As a test scenario, they show as an example the provision of news systems, where the goal is to select appropriate providers according to users' interests. Instead of using content-based filtering in the recommendation process, the reputation of the content provider is used to decide whether or not to ask for news.

Table IX presents the trust dimensions related to the recommendation models, and it provides the answer to the first question, since it is possible to observe the most common dimensions used in the literature according to this type of interaction.

To answer the second question, we realize that most models use witness information as the main information source, and this is due to the fact that the aim of a recommender system is to provide opinions from others. Another important information source that is employed only by Bedi et al. [2007] is sociological information, which is formed by a trust network composed only of reliable agents. In our view, sociological information and witness information are the most relevant information sources to be applied in recommender systems. Additionally, Hermoso et al. [2010] use rules applied in content provision, aiming to standardize the content of the recommended news.

Based on this, we can observe in Table IX that all models are numerical, and this happens because no cognitive reasoning was necessary to get information from witnesses.

We understand that this paradigm is the best suitable for this type of interaction, since agents' confidence is directly related to the ability to provide correct and useful recommendations, often given by a number.

Other important trust dimensions related to this type of interaction are semantics and preferences, and only two models employ these concepts: Bedi et al. [2007] employ semantic and Montaner et al. [2002] employ preferences. In recommender systems, it is important that the user has ways to specify the most important parameters (semantic) and corresponding associated weights (preferences) so the recommender agent can perform better when filtering and returning the results to users.

Hermoso et al. [2010] are the only authors who address the open environment dimension, and we argue that this dimension is one of the most important for recommender systems. It is a surprising fact, since we believe agents from anywhere can make recommendations and improve the decision-making process. Related to this, two models deal with construction of initial trust to newcomers in the system, which is particularly important to recommender systems.

Finally, the third question is discussed taking into account the open environment and the cheating assumption dimensions. We argue that a recommender open MAS should include both dimensions, since it would prevent malicious agents from making recommendations based on their own interests, leaving the user's interests in the background. None of the analyzed models deals with these issues.

5. CONCLUSIONS

The need for interaction is an essential feature in MAS applications. In opened and uncertain environments, agents may present difficulties in obtaining information about unknown members, resulting in a great barrier to interaction. As shown in this article, trust and reputation models still receive attention as the primary alternative to reducing interaction risks in open environments.

This article presented a wide review on computational trust and reputation models for MASs published over the last two decades. We first joined some dimensions presented by authors in the field and discussed the trust and reputation models for MASs based on the selected dimensions. Additionally, we discussed the application of dimensions in the analyzed papers by presenting their use in the models. Afterward, we identified four MASs' types of interaction employed in the analyzed models: coalition, argumentation, negotiation, and recommendation. Based on this, we discussed each one of the models, presenting how they employ trust and reputation mechanisms related to types of interaction. Finally, we presented a set of dimensions related to each type of interaction according to what we have found in the literature and also based on our view about the best set of dimensions for each type of interaction. This analysis can lead to future comparisons and critical analysis about trust and reputation models for MASs, since it will be possible to make comparisons among models and mainly to check if models present the recommended dimensions according to the types of interaction.

The increasing number of trust models makes us reflect on the difficulty of designing a single model that can be used for all types of MAS applications or types of interaction. As we observed, many dimensions must be used to guarantee relevant protection in commercial MASs, depending on the types of interaction. Another difficulty is that most models, even being specific for MASs, do not take into account many features presented in this kind of system.

This article has analyzed hundreds of models that use different strategies depending on the type of environment. Although there is no complete trust model, it is possible to evaluate some alternatives to select a model for a specific application or to build a new one based on the dimensions presented in this article. Additionally, the set of dimensions addressed in this review can assist researchers in the classification of their own models and allow for objectively selecting the necessary dimensions used in the definition of new trust models for MASs. These issues are the main contributions of this article.

REFERENCES

A. Abdul-Rahman and S. Hailes. 2000. Supporting trust in virtual communities. *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Hawaii, USA, 4–7 January 2000, pp. 1–9.

S. Aboulwafa and R. Bahgat. 2010. DiReCT: Dirichlet-based reputation and credential trust management. *Informatics and Systems (INFOS), 2010 The 7th International Conference on*, pp. 1–8, 28–30 March 2010.

Z. M. Aljazzaf, M. Perry, and M. A. M. Capretz. 2010. Online trust: Definition and principles. *Proceedings of the Computing in the Global Information Technology (ICCGI)*. 20–25 Sept. Valencia, Spain: IEEE, 163–168.

L. Amgoud and C. Cayrol. 2002. A reasoning model based on the production of acceptable arguments. *Annals of Mathematics and Artificial Intelligence 34*: 197–216.

D. Artz and Y. Gil. 2007. A survey of trust in computer science and the Semantic Web. *Journal of Web Semantics: Science, Services and Agents on the World Wide Web (2007)*.

R. Ashri, S. D. Ramchurn, J. Sabater, M. Luck, and N. R. Jennings. 2005. Trust evaluation through relationship analysis. In *Proceedings of the 4th International Joint Conference on Autonomous Agents and MultiAgent Systems*, 2005, pp. 1005–1012.

K. S. Barber, K. Fullam, and J. Kim. 2003. Challenges for trust, fraud, and deception research in multi-agent systems. In *Trust, Reputation, and Security: Theories and Practice*, volume 2631 of *LNCS*, pp. 8–14. Springer.

P. Bedi, H. Kaur, and S. Marwaha. 2007. Trust based recommender system for the semantic web. In *IJCAI'07: Proceedings of International Joint Conference on Artificial Intelligence*, pp. 2677–2682, 2007.

J. Bentahar, J. J. C. Meyer, and B. Moulin. 2007. Securing agent-oriented systems: An argumentation and reputation-based approach. In *Proceedings of the 4th International Conference on Information Technology: New Generations (ITNG 2007)*, IEEE Computer Society, pp. 507–515.

C. Bertocco and C. Ferrari. 2008. Context-dependent reputation management for soft security in multi agent systems. In *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligence Agent Technology (WI-IAT'08)*, 9–12 Dec. 2008, Sydney, NSW, Australia, Vol. 3, pp. 77–81.

P. B. Biyela. 2004. Provisioning of secure multi-agent systems (MAS) based on trust contracts. Master's dissertation. Department of Computer Science University of Zululand, South Africa.

M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis. 1999. The role of trust management in distributed system security. In *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*. Vitek and Jensen, Editors, 1999, Springer-Verlag.

J. Borrell, S. Robles, J. Bigham, L. Tokarchuk, and L. Cuthbert. 2001. Design of a trust model for a secure multi-agent marketplace. In *Proceedings of the 5th International Conference on Autonomous Agents*, Montreal, Canada.

V. Botelho, F. Enembreck, B. C. Avila, H. Azevedo, and E. E. Scalabrin. 2009. Encrypted certified trust in multi-agent system. In *Proceedings of the 13th International Conference on Computer Supported Cooperative Work in Design (CSCWD'2009)*, 227–232, Santiago.

C. Burnett, T. J. Norman, and K. Sycara. 2013. Stereotypical trust and bias in dynamic multi-agent systems. *ACM Transaction on Intelligent Systems and Technology (TIST)* 4, 2, 26.

C. Burnett, T. J. Norman, and K. Sycara. 2011. Trust decision-making in multi-agent systems. In *Proceedings of the Twenty Second International Joint Conference on Artificial Intelligence*. 115–120.

J. Carbo, J. Molina, and J. Davila. 2002. Trust management through fuzzy reputation. *International Journal of Coopeative Information Systems* 12, 1, 135–155.

J. Carter and A. A. Ghorbani. 2003. Value centric trust in multiagent systems. In *Proceedings of IEEE/WIC International Conference on Web Intelligence (WI 2003).*

J. Carter, E. Bitting, and A. A. Ghorbani. 2002. Reputation formalization for an information sharing multi-agent system. In *Computational Intelligence* 18, 2, 515–534.

C. Castelfranchi and R. Falcone. 1998. Principles of trust for MAS: Cognitive anatomy, social importance, and quantification. In *Proceedings of 3rd International Conference on MultiAgent Systems*. 72–79.

C. Castelfranchi and R. Falcone. 2001. Social trust: A cognitive approach. In *Trust and Deception in Virtual Societies*, pp. 55–90. Kluwer Academic Publishers.

C. Castelfranchi, R. Falcone, and G. Pezzulo. 2003. Trust in information sources as a source for trust: A Fuzzy approach. In *Proceedings of the Second International Joint Conference on Automonous Agents and Multiagent Systems (AAMAS)*, ACM Press, New York, USA, pp. 89–96.

A. M. Chopra, E. Paja, and P. Giorgini. 2011. Sociotechnical trust: An architectural approach. In *Proceedings Conference Conceptual Modeling, LNCS 6998*, pp. 104–117.

R. Conte and M. Paolucci. 2002. Reputation in artificial societies: Social beliefs for social order. Kluwer Academic Publishers.

M. Daignault, M. Shepherd, S. Marche, and C. Watters. 2002. Enabling trust online. In *Proceedings of the 3rd International Symposium on Electronic Commerce (ISECí02)*. 3–12.

A. Das and M. M. Islam. 2012. SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems. In *IEEE Transactions on Dependable and Secure Computing* 9, 2, 261–274.

G. Derbas, A. Kayssi, H. Artail, and A. A. Chehab. 2004. TRUMMAR - A trust model for mobile agent systems based on reputation. In *IEEE/ACS International Conference on Pervasive Services (ICPS)*, pp. 113–120.

P. Dondio and S. Barret. 2007. Presumptive selection of trust evidence. In *Proceedings of the 6th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS'07)*, E. H. Durfee, M. Yokoo, M. N. Huhns, and O. Shehory, Eds., 2007, p. 166.

R. I. M. Dunbar. 1998. The social brain hypothesis. *Evolutionary Anthropology* 6, 178–190.

M. duPreez. 2009. Trust and new technologies: Marketing and management on the Internet and Mobile media. *Online Information Review*. Vol. 33 Iss: 6, 1208–1209. Emerald Group Publishing Limited.

eBay. 2015. http://www.ebay.com.

N. E. Elgohary, A. A. Elfetouh, and S. I. Barakat. 2010. Developing a reputation model for electronic markets. *International Journal of Electrical and Computer Science (IJECS-IJENS)* 10, 6.

E. Erriquez, V. D. Hock, and M. Wooldridge. 2011. An abstract framework for reasoning about trust. In *Proceedings of the Tenth International Conference on Autonomous Agents and MultiAgent Systems (AAMAS'2011)*. 1085–1086.

H. Fang, J. Zhang, and N. M. Thalmann. 2013. A trust model stemmed from the diffusion theory for opinion evaluation. In *Proceedings of the 12th International Joint Conference on Autonomous Agents and MultiAgent Systems (AAMAS'2013)*, St. Paul, MN, pp. 805–812.

H. Fang, J. S. M. Zhang, and M. N. Thalmann. 2012. Sarc: Subjectivity alignment for reputation computation. In *Proceedings of the 11th International Joint Conference on Autonomous Agents and MultiAgent Systems*. 1365–1366.

J. Ferber. 1999. Multi-agent systems: An introduction to distributed artificial intelligence. Addison-Wesley.

T. Finin and A. Joshi. 2002. Agents, trust, and information access on the semantic web. *ACM SIGMOD Rec.*, 31, 4, 30–35, Dec. 2002.

K. Fullam, T. B. Klos, G. Muller, J. Sabater, A. Scholosser, Z. Topol, K. S. Barber, J. S. Rosenshein, L. Vercouter, and M. Voss. 2005. A specification of the agent and reputation trust (art) testbed: Experimentation and competition for trust in agent societies. In *Proceedings of the 4th International Joint Conference on Autonomous Agents and MultiAgent Systems (AAMAS'05)*, pp. 512–518. ACM Press, July 2005.

D. Gambetta. 1988. Can We trust Trust? In *Trust: Making and Breaking Cooperative Relations*, Basil Blackwell, New York, pp. 213–237.

R. Ghanea-Hercock. 2007. Dynamic trust formation in multi-agent systems. In *Tenth International Workshop on Trust in Agent Societies at the Autonomous Agents and Multi-Agent Systems Conference*, Hawaii.

T. Grandison and M. Sloman. 2000. A survey of trust in internet applications. *IEEE Communications Surveys and Tutorials* 4, 4, 2–16.

N. Griffiths and M. Luck 2003. Coalition formation through motivation and trust. In *Proceedings of the 2nd International Conference on Autonomous Agents and MultiAgent Systems (AAMAS'03)*. 17–24.

N. Griffiths. 2005. Task delegation using experience-based multi-dimensional trust. In *Proceedings of the 4th International Joint Conference on Autonomous Agents and MultiAgent Systems (AAMAS'05)*, ACM Press, pp. 489–496.

V. S. Grishchenko. 2004. A fuzzy model for context-dependent reputation. In *Proceedings of Trust, Security and Reputation Workshop at ISWC 2004*, Hiroshima, Japan.

A. Gutowska and K. Buckley. 2008. Computing reputation metric in multi-agent e-commerce reputation system. In *IEEE International Conference on Distributed Computing Systems Workshops*, 255–260. IEEE, Los Alamitos.

Y. Haghpanah and M. desJardins. 2012. PRep: A probabilistic reputation model for biased societies. In *Proceedings of the 11th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS'12)*. 315–322.

R. Hermoso, H. Bilhardt, and S. Ossowski. 2010. Role evolution in open multi-agent systems as an information source for trust. In *Proceedings of 9th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS'10)*.

H. Huang, G. Zhu, and A. Jin. 2008. Revisiting trust and reputation in multi-agent systems. In *ISECS International Colloquium on Computing, Communication, Control, and Management*, Guangzhou, China, pp. 424–429.

F. K. Hussain, E. E. Chang, and O. Hussain. 2008. A robust methodology for prediction of trust and reputation values. In *Proceedings of the ACM Conference on Computer and Communications Security*. 97–108.

T. D. Huynh, N. R. Jennings, and N. R. Shadbolt. 2006. Certified reputation: How an agent can trust a stranger. In *Proceedings of the Fifth International Joint Conference on Autonomous Agents and Multi-Agent Systems*. 1217–1224.

T. D. Huynh, N. R. Jennings, and N. R. Shadbolt. 2004. FIRE: An integrated trust and reputation model for open multi-agent systems. In *Proceedings of the 16th European Conference on Artificial Intelligence (ECAI)*. 18–22.

D. Johnson-George and R. Swap 1982. Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other. *Journal of Personality and Social Psychology* 43, 1306–1317.

A. Josang and R. Ismail. 2002. The beta reputation system. In *Proceedings of the 15th Bled Electronic Commerce Conference*, June 2002.

A. Josang. 1996. The right type of trust for distributed systems. In *Proceeding of the 1996 Workshop on New Security Paradigms*, Lake Arrowhead, USA, 16–19 September 1996, pp. 119–131.

R. Jurca and B. Faltings. 2003. An incentive compatible reputation mechanism. In *Proceedings of the 6th International Workshop on Deception Fraud and Trust in Agent Societies (at AAMAS'03)*, ACM.

S. N. L. C. Keung and N. Griffiths. 2008. Using recency and relevance to assess trust and reputation. In *Proceedings of AISB 2008 Symposium on Behaviour Regulation in Multi-Agent Systems.* The Society for the Study of Artificial Intelligence and Simulation of Behaviour 4, pp. 13–18.

B. Khosravifar, J. Bentahar, M. Gomrokchi, and R. Alam. 2012. CRM: An efficient trust and reputation model for agent computing. Knowledge-Based Systems, in press. DOI: http://dx.doi.org/10.1016/j.knosys.2011.01.004

B. Khosravifar, M. Gomrokchi, J. Bentahar, and P. Thiran. 2009. Maintenance-based trust for multi-agent systems. In *Proceedings of the 8th International Conference on Autonomous Agents and MultiAgent Systems*. 1017–1024.

H. Klabi, K. Mellouli, S. Mellouli, and M. Rekik. 2012. A trust model for a multi-agent negotiation. In *Proceedings of the International Conference on Communications and Information Technology (ICCIT'12)*. 291–296, June 2012.

L. Klejnowski, Y. Bernard, J. Hähner, and C. M. Schloer. 2010. An architecture for trust-adaptive agents. In *Proceedings of the 2010 Fourth IEEE International Conference on Self-Adaptive and Self-Organizing Systems Workshop (SASOW)*, IEEE Computer Society Press.

A. Koster, J. Sabater, and M. Shorlemmer. 2011. Personalizing communication about trust. In *Proceedings of the Eleventh International Conference on Autonomous Agents and Multiagent Systems (AAMAS'12)*, pp. 655–664. IFAAMAS, Valencia, Spain.

A. Koster, M. Schorlemmer, and J. Sabater. 2013. Opening the black box of trust: Reasoning about trust models in a bdi agent. *Journal of Logic and Computation* 23, 1, 25–58.

D. M. Kreps and R. Wilson. 1982. Reputation and imperfect information. *Journal of Economic Theory*, volume 27, Elsevier Science, USA, 253–279

G. Lei, W. Xiaolin, and Z. Guangzhou. 2009. Trust-based optimal workplace coalition generation. In *Information Engineering and Computer Science (ICECS'09), International Conference on*, pp. 1–4.

B. Li, M. Xing, J. Zhu, and T. Che 2008. A dynamic trust model for the multi-agent systems. In *Proceedings of IEEE International Symposiums on Information Processing (ISIP'08)*. 500–504.

L. Li, H. Li, G. Lu, and S. Yao. 2007. A quantifiable trust model for multi-agent system based on equal relations. In *IEEE Computer: International Conference on Computational Intelligence and Security.*

X. Liu and A. Datta. 2011. A trust prediction approach capturing agent's dynamic behaviour. In *Proceedings of the 22nd International Joint Conference on Artificial Intelligence (IJCAI'11).*

S. Liu, A. C. Kot, C. Miao, and Y. Theng. 2012. A Dempster-Shafer theory based witness trustworthiness model to cope with unfair ratings in e-marketplace. In *Proceedings of the 14th Annual International Conference on Electronic Commerce*. 99–106.

S. Liu, H. Yu, C. Miao, and A. C. Kot. 2013a. A fuzzy logic based reputation model against unfair ratings. In *Proceedings of the 2013 International Conference on Autonomous Agents and Multi-agent Systems*. 821–828.

X. Liu, A. Datta, and K. Rzadca. 2013b. Trust beyond reputation: A computational trust model based on stereotypes. *Journal of Electronic Commerce Research and Applications* 12, 24–39.

S. Liu, J. Zhang, C. Miao, Y. L. Theng, and K. C. Alex. 2011. iCLUB: An integrated clustering-based approach to improve the robustness of reputation systems (extended abstract). In *Proceedings of the Tenth International Joint Conference on Autonomous Agents and Multiagent Systems*. 1151–1152.

X. Liu and A. Datta. 2012. Modeling context aware dynamic trust using hidden Markov model. In *Proceedings of the 26th AAAI Conference on Artificial Intelligence (AAAI'12)*. 1938–1944.

G. Lu, J. Lu, S. Yao, and J. Yip. 2009. A review on computational trust models for multi-agent systems. In *International Conference on Internet Computing*, pp. 325–331.

N. Luhmann. 2000. Familiarity, confidence, trust: Problems and alternatives. In *Trust: Making and Breaking Cooperative Relations*, Basil Blackwell, New York, pp. 94–107.

P. A. Matt, M. Morge, and F. Toni. 2010. Combining statistics and arguments to compute trust. In *Proceedings of the 9th International Conference on Autonomous Agents and MultiAgent Systems*, pp. 209–216, Toronto, Canada.

S. P. Marsh. 1994. Formalizing trust as computational concept. PhD Thesis, University of Stirling.

D. J. McAllister. 1995. Affect and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal* 38, 1, 24–59.

M. Montaner, B. López, and J. L. Rosa de la. 2002. Developing trust in recommender agents. In *Proceedings of the first International Joint Conference on Autonomous Agents and MultiAgent Systems (AAMAS'02)*. 304–305, Bologna, Italy.

E. Mokhtari, Z. Noorian, B. T. Ladani, and M. A. Nematbakhsh. 2011. A context-aware reputation-based model of trust for open multi-agent environments. In *Advances in Artificial Intelligence*, pp. 301–312. Springer Berlin Heidelberg.

M. R. Mokhtar, U. Wajid, and W. Wang. 2007. Collaborative trust in multi-agent system. In *16th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2007)*, 30–34.

L. Mui. 2002. A computational model of trust and reputation: Agents, evolutionary games, and social networks. Ph.D. thesis, Massachusetts Institute of Technology.

L. Mui, M. Mihtashemi, and A. Halberstadt. 2002. Notions of reputation in multi-agents systems: A review. *Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent System (AAMAS 2002)*, Bologna, Italy, 15–19 July 2002, pp. 280–287.

G. Muller and L. Vercounter. 2005. Decentralized monitoring of agent communications with a reputation model (LIAR). In *Trusting Agents for trusting Electronic Societies, Lecture Notes in Computer Sciense*, 144–161.

B. Neville and J. Pitt. 2004. A computational framework for social agents in agent mediated e-commerce. In *Proceedings of the Seventh International Workshop on Trust in Agent Societies,* R. Falcone, S. Barber, L. Korba, and M. Singh, Eds., New York, July 2004, 83–91.

M. A. S. N. Nunes. 2011. Computação Afetiva personalizando interfaces, interações e recomendações de produtos, serviços e pessoas em ambientes computacionais. In Portfólio DCOMP. EditoraUFS.

N. T. Nkosi, M. O. Adigun, and J. O. Emuoyibofarhe. 2007. Agent-to-agent reputation-based trust management. *IADIS International Conference Applied Computing*, pp. 143–150.

B. Padovan, S. Sackmann, T. Eymann, and I. Pippow. 2001. A prototype for an agent-based secure electronic marketplace including reputation-tracking mechanisms. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences (HICSS-34)*, 2235–2244, Maui, Hawaii – Track 7, January 3–6 2001.

S. Parsons, Y. Tang, E. Sklar, P. McBurney, and Cai. K. 2011. Argumentation-based reasoning in agents with varying degrees of trust. In *Proceedings of the 10th International Conference on Autonomous Agents and MultiAgent Systems*. 879–886.

S. A. Pinto. 2008. Simulação e Avaliação de Comportamentos em Sistemas Multi-Agentes baseados em Modelos de Reputação e Interação. UNISINOS - Computação Aplicada (PIPCA) – RS /USP – ICMC, SP – Brazil.

I. Pinyol and J. Sabater. 2013. Computational trust and reputation models for open multi-agent systems: A review. *Artificial Intelligence Review.* DOI: 10.1007/s10462-011-9277-z

I. Pinyol, M. Sabater, P. Dellunde, and M. Paolucci. 2012. Reputation-based decisions for logic-based cognitive agents. *Autonomous Agents and Multi-Agent Systems* 24, 1, 175–216.

M. Piunti, M. Venanzi, C. Castelfranchi, and R. Falcone. 2012. Multimodal trust formation with uninformed cognitive maps (UnCM). In *Proceedings the 11th Conference on Autonomous Agents and MultiAgent Systems* 3, pp. 1241–1242.

S. D. Ramchurn, N. R. Jennings, C. Sierra, and L. Godo. 2004a. Devising a trust model for multi-agent interactions using confidence and reputation. *Applied Artificial Intelligence*, 18, 9–10, 833–852.

S. D. Ramchurn, D. Huynh, and N. R. Jennings. 2004b. Trust in multi-agent systems. *The Knowledge Engineering Review* 19, 1, 1–25.

S. Reece, A. Rogers, S. Roberts, and N. R. Jennings. 2007. A multidimensional trust model for heterogeneous contract observation. In *Proceedings of the 22nd AAAI Conference on Artificial Intelligence.* AAAI Press, Vancouver, British Columbia, Canada, pp. 128–135.

S. Reches, P. Hendrix, S. Kraus, and B. J. Grosz. 2008. Efficiently determining the appropriate mix of personal interaction and reputation information in partner choice. In *Proceedings of 7th International Conference on Autonomous Agents and Multiagent Systems (AAMAS'08)*. 583–590.

K. Regan, P. Poupart, and R. Cohen. 2006. Bayesian reputation modeling in e-marketplaces sensitive to subjectivity, deception and change. In *Proceedings of the Conference on Artificial Intelligence (AAAI'06)*. 1206.

M. Rehák, L. Foltyn, M. Pechoucek, and P. Benda. 2005. Trust model for open ubiquitous agent systems. In *Intelligent Agent Technology, IEEE/WIC/ACM International Conference*, number PR2416 inIEEE.

A. Rettinger, M. Nickles, and V. Tresp. 2008. A statistical relational model for trust learning. In *Proceedings of the 7th International Conference on Autonomous Agents and Multiagent Systems*, pp. 763–770. Estoril, Portugal.

A. Rettinger, M. Nickles, and V. Tresp. 2007. Learning initial trust among interacting agents. *Lecture Notes in Computer Science*, 4676, 313–327.

D. Rosaci, G. M. L. Sarne, and S. S. Garruzzo. 2012. Integrating trust measures in multiagent systems. *International Journal of Intelligent Systems* 27, 1, 1–15.

D. Rosaci. 2012. Trust measures for competitive agents. *Knowledge-based Systems*, 28, 38–46.

J. C. Rubiera, J. M. M. Lopez, and J. D. Muro. 2001. A fuzzy model of reputation in multi-agent systems. In *Proceedings of the 5th International Conference on Autonomous Agents.* ACM Press, pp. 25–26.

J. Sabater, M. Paolucci, and R. M. Conte. 2006. Repage: REPutation and ImAGE among limited autonomous partners. *Journal of Artificial Societies and Social Simulation* 9, 2.

J. Sabater and C. Sierra. 2002. Reputation and social network analysis in multi-agent systems. In *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. 475–482, Bologna, Italy.

J. Sabater and C. Sierra. 2005. Review on computational trust and reputation models. *Artificial Intelligence Review* 24, 1, 33–60.

A. Salehi-Abari and T. White. 2012. DART: A distributed analysis of reputation and trust framework. *Computational Intelligence*, 28, 642–682. DOI: 10.1111/j.1467-8640.2012.00453.x

M. Schillo, P. Funk, and M. Rovatsos. 2000. Using trust for detecting deceitful agents in artificial societies. *Apllied Artificial Intelligence Journal* (Special Issue on Trust, Deception and Fraud in Agent Societies).

S. Sen and N. Sajja. 2002. Robustness of reputation-based trust: Boolean case. In *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. 288–293, Bologna, Italy.

E. Serrano, M. Rovatsos, and J. Botia. 2012. A qualitative reputation system for multiagent systems with protocol-based communication. In *Proceedings of the 11th Conference on Autonomous Agents and Multiagent Systems* 1, pp. 307–314.

N. K. Sharma, V. Gaur, and S. K. Muttoo. 2012. A dynamic reputation system with built-in attack resilience to safeguard buyers in e-market. *ACM SIGSOFT Software Engineering Notes* 37, 4, 1–19.

J. Shi, G. V. Bochmann, and C. Adams. 2005. Dealing with recommendations in a statistical trust model. In *Proceedings of the Workshop on Trust in Agent Societies at AAMAS 2005*. 144–155, Utrecht.

P. M. Singh. 2011. Trust as dependence: A logical approach. In *Proceedings of the 10th International Conference on Autonomous Agents and Multiagent System (AAMAS'11)*. 863–870.

C. Sierra and J. Debenham. 2005. An information-based model for trust. In *Proceedings of 4th International Joint Conference on Autonomous Agents and Multiagent Systems*, 497–504. Uterecht, The Nederlands.

W. Song, V. V. Phoha, and X. Xu. 2004. An adaptive recommendation trust model in multiagent system. In *IAT, IEEE Computer Society*, pp. 462–465.

X. Su, M. Zhang, Y. Mu, and Q. Bai. 2013. A robust trust model for service-oriented systems. *Journaul of Computer and System Sciences* 79, 5, 596–608.

A. Sutcliffe and D. Wang. 2012. Computational modelling of trust and social relationships. *Journal of Artificial Societies and Social Simulation* 15, 1, 3.

L. T. W. Teacy, M. Luke, A. Rogers, and R. N. Jennings. 2012. An efficient and versatile approach to trust and reputation using hierarchical bayesian modeling. *Artificial Intelligence* 193, 149–185.

W. T. L. Teacy, G. Chalkiadakis, A. Rogers, and N. R. Jennings. 2008. Sequential decision making with untrustworthy service providers. In *Proceedings of the 7th International Conference on Autonomous Agents and Multiagent Systems*. 755–762.

W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck. 2006. TRAVOS: Trust and reputation in the context of inaccurate information sources. *Autonomous Agents and Multiagent Systems* 12, 2, 183–198.

J. Tian, J. Li, and L. Yanga. 2009. Reputation-based multi-agent model for network resource selection. *International J. Communications, Network and System Sciences*, 2, 764–774, DOI:10.4236/ijcns.2009.28089

X. Tong, H. Huang, and W. Zhang. 2009. Agent long-term coalition credit. *Expert Systems with Applications: An International Journal* 36, 5, 9457–9465.

T. Tran and R. Cohen. 2004. Improving user satisfaction in agent based electronic marketplaces by reputation modelling and adjustable product quality. In *Proceedings of the Third International Joint Conference on Autonomous Agents and Mutiagent Systems (AAMAS'04)*. 828–835, New York, USA.

A. Urzica, H. A. Mogos, and M. A. Florea. 2011. A reputation based negotiation model for barter transactions between software agents. *International Journal on Artificial Intelligence Tools* 20, 1001.

A. Urzica. 2010. Distributed reputation extraction in multi-agent systems. In *Proceedings of the 12th European Agent Systems Summer School Student Session*. 5–11.

M. Venanzi, M. Piunti, R. Falcone, and C. Castelfranchi. 2011. Facing openness with socio cognitive trust and categories. In *Proceedings the 22nd International Joint Conference on Artificial Intelligence (IJCAI)*, Barcelona, Spain, 16-22 Jul 2011. AAAI Press, pp. 400–405.

G. Vogiatzis, I. MacGillivray, and M. Chli. 2010. A probabilistic model for trust and reputation. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems*. 225–232.

G. Wang and X. Gui. 2013. Dynamic recommendation trust model based on information entropy and heuristic rules in e-commerce environment. *Electronics and Electrical Engineering* 19, 4, 71–76.

P. Wang and Z. Zhang. 2005. A computational trust model with trust network in multi-agent systems. *Proceedings of the 2005 International Conference on Active Media Technology (AMT2005)*, May 19–21, 2005, Kagawa International Conference Hall, Takamatsu, Kagawa, Japan, IEEE Xplore, Piscataway, N.J, pp. 389–392.

Y. Wang, M. Li, E. Dillon, L. G. Cui, J. J. Hu, and L. J. Liao. 2008. A context-aware computational trust model for multi-agent systems. In *Networking, Sensing and Control (ICNSC'2008). IEEE International Conference on*, 1119–1124.

Y. Wang and J. Vassileva 2003. Trust and reputation model in peer-to-peernetworks. *Proceedings of the 3rd IEEE International Conference on Peer-to-Peer Computing*, Linköping, Sweden; 1–3 September 2003, pp. 150–158.

P. William. 1992. Prisoner's Dilemma: John Von Neumann, Game Theory and the Puzzle of the Bomb. Doubleday, New York, NY, USA.

M. Wooldridge. 2009. An Introduction to MultiAgent Systems. Department of Computer Science, University of Liverpool, UK. John Wiley & Sons, LTD.

R. Yaich, O. Boissier, P. Jaillon, and G. Picard. 2011. Social-compliance in trust management within virtual communities. In *3rd International Workshop on Web Intelligence and Intelligent Agent Technology (WI-IAT'2011).*

B. Yu and M. P. Singh. 2003. Detecting deception in reputation management. In *Proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. ACM, 73–80.

H. Yu, Z. Shen, C. Leung, C. Miao, and V. R. Lesser. 2013. A survey of multi-agent trust management systems. *IEEE Access* 1, 1, 35–50.

W. Yu, Y. Univ, Yangzhou, Z. Qiuyue, and J. Ying. 2008. A trust management model based on multi-agent system. *Computing, Communication, Control, and Management (CCCM'08), ISECS International Colloquium on*, pp. 449–453.

L. You. 2007. An adaptative reputation-based trust model for intelligent agents in e-market place. Doctoral Dissertation, University of Texas at Arlington, USA.

J. Zhang, A. A. Ghorbani, and R. Cohen. 2007. A familiarity-based trust model for effective selection of sellers in multiagent e-commerce systems. *International Journal of Information Security* 6, 5, 333–344.

X. Zheng, Z. Wu, H. Chen, and Y. Mao. 2006. Developing a composite trust model for multi-agent systems. In *Proceedings of the Fifth International Joint Conference on Autonomous Agents and Multiagent Systems*, Hakodate, Japan.

Q. Zhou, C. Wang, and J. Xie. 2009. Core: A trust model for agent coalition formation. *Fifth International Conference on Natural Computation (ICNC'09)* 5, 541–545.

Received February 2014; revised June 2015; accepted August 2015