Survey on Computational Trust and Reputation Models

DIEGO DE SIQUEIRA BRAGA, MARCO NIEMANN, and BERND HELLINGRATH,
University of Muenster—ERCIS, Germany
FERNANDO BUARQUE DE LIMA NETO, University of Pernambuco, Brazil

Over the recent years, computational trust and reputation models have become an invaluable method to improve computer-computer and human-computer interaction. As a result, a considerable amount of research has been published trying to solve open problems and improving existing models. This survey will bring additional structure into the already conducted research on both topics. After recapitulating the major underlying concepts, a new integrated review and analysis scheme for reputation and trust models is put forward. Using highly recognized review papers in this domain as a basis, this article will also introduce additional evaluation metrics to account for characteristics so far unstudied. A subsequent application of the new review schema on 40 top recent publications in this scientific field revealed interesting insights. While the area of computational trust and reputation models is still a very active research branch, the analysis carried out here was able to show that some aspects have already started to converge, whereas others are still subject to vivid discussions.

CCS Concepts: • **General and reference** → *Surveys and overviews*; • **Information systems** → **Reputation systems**; • **Security and privacy** → **Trust frameworks**; • **Computing methodologies** → *Knowledge representation and reasoning*; Intelligent agents;

Additional Key Words and Phrases: Computational trust, reputation management systems

ACM Reference format:
Diego de Siqueira Braga, Marco Niemann, Bernd Hellingrath, and Fernando Buarque de Lima Neto. 2018. Survey on Computational Trust and Reputation Models. *ACM Comput. Surv.* 51, 5, Article 101 (November 2018), 40 pages.
https://doi.org/10.1145/3236008

1 INTRODUCTION

In the past few decades, a considerable amount of research has been conducted on the topics of computational trust and reputation models[1] (Ahmad 2012; Burnett 2011; Teacy et al. 2012; Tian et al. 2016; Urbano et al. 2011; Yu et al. 2013). Studying underlying ideas such as trust (*between humans*) had gained prominence long before interest in the computational aspects appeared (Kini and Choobineh 1998). One of the starting points for considering computers and trust in the same context was Marsh's Ph.D. Thesis (Marsh 1994), which is deemed to be the first publication merging these two concepts.

Authors' addresses: D. de Siqueira Braga, M. Niemann, and B. Hellingrath, University of Muenster—ERCIS, Leonardo-Campus 3, Muenster, 48149, Germany; emails: {diego.siqueira, marco.niemann, bernd.hellingrath}@ercis.uni-muenster.de; F. B. de Lima Neto, University of Pernambuco, R. Benfica, 455 - Madalena, Recife - PE, 50720-001, Brazil; email: fbln@ecomp.poli.br.

0360-0300/2018/11-ART101 $15.00
https://doi.org/10.1145/3236008

Research regarding (computational) trust and reputation has not only been conducted with regard to supply chains, e-commerce, or Information Systems but also spans a wide variety of different academic disciplines, including psychology, economics, and sensor networks (Ashtiani and Azgomi 2014; Brinkhoff et al. 2015; Grandison and Sloman 2000; Mui et al. 2002a, 2002b; Pinyol and Sabater-Mir 2013b; Sabater and Sierra 2005). Many practical approaches on high-profile applications are still currently in intensive use. For example, the reputation systems on websites like eBay, Amazon, or individual rating websites such as Tripadvisor and Goodreads. Accordingly, trusting relationships have been discovered and described between various entities including between IT-systems, humans, and/or organizations (Laeequddin et al. 2010).

Given the need for answers to tackle the given challenges, both research and practice have begun to develop theoretical models to get a better understanding of the domain, as well as practical solutions to support the affected entities. Despite the already existing large array of research, authors continue to propose new models and ideas, thus making this research area a trending, still incomplete, and inconsistent topic (Jøsang 2007; Jøsang et al. 2007; Pinyol and Sabater-Mir 2013b).

To frame the conducted research in some systematic order, a variety of survey papers have been published. An earlier study carried out by Sabater and Sierra (2005), tried to compile an overview of the already existing computational trust and reputation methods present in the literature. More recently, similar undertakings have been executed by Ruohomaa et al. (2007), Lu et al. (2009), Yu et al. (2013), and Pinyol and Sabater-Mir (2013b), as a non-complete but representative sample.

As the research domain is still evolving, new concepts emerge, including novelties such as e-trust (compare statements by Deutsch (1958) and research results of Laeequddin et al. (2010)). Thus, to avoid the risk of missing what has recently been researched, and what is currently considered state of the art in such a fast paced research domain motivated us to systematically review research efforts from the years 2013 to 2016, especially considering the fact that the last major literature review was published in 2013. As a consequence, this survey will try to be the required additional guidance through these recent developments. To achieve this goal, Section 2 presents an extensive overview of the concepts of trust and reputation, as well as their computational offspins. Section 3 contains the conceived evaluation matrix, which integrates several already known and implemented schemes that can be used to classify and analyze trust and reputation models. In Section 4 the new approach is used on a set of recent research approaches (the selection is also described in Section 3). Overall takeaways and results are then discussed in the concluding Section 6.

As a design decision, this survey has a special focus on assessing computational models that allow follow-up implementations.

2 DEFINITIONS AND BACKGROUND

2.1 Definition(s) of Trust

The first element that needs to be discussed when talking about "*Computational Trust and Reputation models*" is the concept of trust. This seems appropriate considering the widespread assumption that trust is an important concept for business/commercial relationship (*between individuals but also between larger institutions*) (Clark and Lee 1999; Dellarocas 2003; Grandison and Sloman 2000; McKnight and Chervany 2001; Sabater and Sierra 2005). While most of these papers focus on business in general, the discussion is also ongoing in the area of Supply Chain Management. One article by Laeequddin et al. (2010) sums up much of the related discussion and the importance of getting alright, the concepts of trust.

Despite its apparent importance, trust remains a difficult concept to grasp and define properly. Deutsch (1958) indirectly mentions this problem pointing out that up to that moment, no sufficient

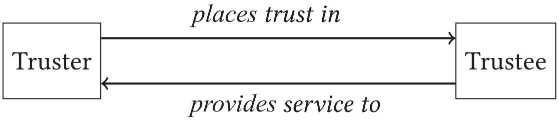


Fig. 1. The relationship between trustee and truster.

(experimental) research had been conducted. Half a century later, still no standard definition exists, leading to a variety of different definitions throughout Academia (for an overview, see Laeequddin et al. (2010)), and some practical examples, see Schwieters (2015). Commonly mentioned reasons for that ambiguity include: trust being "complex" (McKnight and Chervany 2001), "abstract" (Schwieters 2015), and "confusing" (Shapiro 1987). This is aggravated by the fact that trust is not a stable but rather a dynamic concept, as Botsman (2015, 2016) points out in some of her articles.

Yet, despite the variety of existing definitions and the difficulties in finding a standard one, there are some elements that most authors can agree on. One common concept is visualizing trusting as the relationship between a so-called Truster and a Trustee (see Figure 1). As depicted in Figure 1, the truster is the party that is in need of some service and thus places his/her trust into the trustee, a second entity who is supposed to provide the required service (Laeequddin et al. 2010). Here it has to be noted that the relationship does not necessarily have to be a 1:1 one, but could also be 1:n/n:n/n:1, depending on the situation (Grandison and Sloman 2000). Furthermore, it is important to understand that the relationship between the two entities is not required to be symmetric (Grandison and Sloman 2000).

Another often-mentioned property of trust is its context dependence. Sabater and Sierra (2005) explain this with a basic example. They point out that a doctor would be trusted when it comes to medical treatment but might not be trusted when a suggestion for a bottle of wine was needed. Grandison and Sloman (2000) put it differently by pointing out that trust was not absolute, meaning that no trustee would be trusted in every potential situation. They also add that trust in itself usually underlies the very same limitations. The only notable exception here is Zhong et al. (2015), who distinguish between competence (*trust in expertise*) and integrity (*trust in goodwill*) trust and classify integrity trust as a non-context dependent.

A third necessary property of trust, respectively, for the need for trust, is the existence of uncertainty and risks (Laeequddin et al. 2010; McKnight and Chervany 2001). The reason behind this is that with complete information trust would not be required (Laeequddin et al. 2010). Based on the definition of trust given by Deutsch (1958), Kini and Choobineh (1998) add that usually, the negative consequences (*induced by risk and uncertainty*) of trust should outweigh the potential positive outcomes. In sum, they state that trust always leads to a state of vulnerability.

The last rather commonly shared perception about trust is the fact that in current research it is considered to be multidimensional (Kini and Choobineh 1998; McKnight and Chervany 2001; Sabater and Sierra 2005). As Sabater and Sierra (2005) correctly observe, it is, among other things, these different dimensions or perspectives that create difficulties when discussing trust. To illustrate the span of different dimensions/perspectives of trust, the respective schema from a selection of papers is presented in Table 1.

As Table 1 shows, the differences are the majority. However, there are at least some similarities, as Lee and Moray (1992) talk about performance and Schwieters (2015) about effectiveness. Other mentioned similarities are competence and predictability, which are referred to by both Grandison and Sloman (2000) and Muir (1987). Since comparing each element to come up with a new and more precise trust definition is beyond the scope of this article, this subsection should be understood as a general introduction to the trust concept.

Table 1. Examples of Trust Dimensions/Perspectives/Characteristics

Paper	Dimensions/Perspectives/Characteristics
Sabater and Sierra (2005)	conceptual model, information sources, visibility types, model's granularity, agent behavior assumptions, type of exchanged information, trust/reputation reliability measure
Grandison and Sloman (2000)	access to trustor's resources, provision of service by trustee, certification of trustees, delegation, infrastructure test
McKnight and Chervany (2001)	competence, predictability, benevolence, integrity, other
Schwieters (2015)	legitimacy, transparency, effectiveness
Kini and Choobineh (1998)	individual trust, societal trust, relationship trust
Muir (1987)	expectations of trust (*persistence, technical competence, fiduciary responsibility*), dynamics of trust (*predictability, dependability, faith*)
Lee and Moray (1992)	purpose, process, performance, foundation

2.2 Computational Trust—Definition and Contrast to the Traditional Trust Concept

The general concept of trust described earlier can be intuitively applied to relationships between humans and partly also to human-computer or even to computer-computer relationships. Even though social trust is considered to be an emotive issue, and since machines fall short on emotional aspects, a more formal/rational model is required (Marsh 1992). Nevertheless, the notion of computational trust is derived from real world trust as a sufficient actual tested concept (Marsh 1992)—or as (Sassone et al. 2007) put it: "*an abstraction inspired by the human concept of trust.*"

The first attempt to create a corresponding model in the area of computer science was conducted by Marsh (1994), who published a first sketch of his approach two years earlier (Marsh 1992). He introduced mathematical expressions of necessary trust components and expressed trust concepts by *formulae* together with thresholds usable for decision making (Marsh 1992).

Since then many diverse new models have been proposed, as it can be seen in an aggregated manner in papers like the ones by Pinyol and Sabater-Mir (2013b) and Sabater and Sierra (2005). With the new models come additional computational issues, like social networks or Human-Computer Interaction (HCI)/Human-Robot Interaction (HRI), and were included as potential application areas (Sassone et al. 2007).

At this point, it appears to be of importance mentioning that computational trust models are not solely developed to make the Internet more secure. Intuitively, the Internet often is still connected with the assumption of human peers playing a role in the overall interaction. However, computational trust models (*at least some*) are also developed to be used in entirely artificial environments, such as Multi-Agent System (MAS) or Distributed Artificial Intelligence (DAI) (Marsh 1992, 1994). The underlying reasoning is that each society (including virtual ones) would require trust to function. An interesting remark in that regard is provided by Abdul-Rahman and Hailes (2000), who point out that each society in the end was bound to humans, meaning that software agents serve people by delivering a result. Thus, using similar reasoning, models appear to be even more desirable.

2.3 Definition(s) of Reputation

The second element that requires definition is the concept of reputation. Being discussed second does not imply reputation being of less relevance than trust but solely accounts for the positioning in this article's title. While most of the existing reputation-related papers deal with commerce and e-commerce (Franke et al. 2005; Houser and Wooders 2006; Resnick and Zeckhauser 2002), Supply Chain Management is also discussed as one area that can benefit from the use of reputation mechanisms (Franke et al. 2005). Greco et al. (2011) even made an interesting point that a good reputation mechanism would bring simulations closer to reality—a high desirability characteristic for such models.

Unfortunately, reputation suffers from the same problem as trust, by lacking a precise definition commonly used throughout the literature. Mui et al. (2002b) even explicitly stated that reputation is an intuitive concept. While this may not be incorrect, intuition fails to deliver an objective characterization once again making many different definitions available.

Fortunately and similar to trust, several notions can be observed throughout vast areas of the existent literature—some even being related to some aspects from the trust section. The first is a rather general definition presented in several papers, which points out that reputation can be understood as the perception an agent/the public has of another agent (Kravari and Bassiliades 2016; Mui et al. 2002b), which is used to choose a cooperation partner (Pinyol and Sabater-Mir 2013b). More precisely, this comes down to memorizing and using the past actions of an agent to predict its potential future behavior (Kollock 1999; Ruohomaa et al. 2007). The underlying intention is to reduce existing information asymmetries, as described by Akerlof (1970), by using reputation as a tool for risk (Kollock 1999) and complexity (Abdul-Rahman and Hailes 2000) management.

The social aspect is the second component that is prevalent in papers dealing with reputation. For example, Mui et al. (2002a) call reputation a social concept, and Pinyol and Sabater-Mir (2013b) and Abdul-Rahman and Hailes (2000) denote reputation as a social control artifact. A slightly more detailed version of reputation as a social control mechanism is presented by Zacharia et al. (1999), who explain that reputation was developed by social interaction between members of a loosely coupled group with similar interests. Reputation's deep roots in an ancient societal context also become evident in the following facts: First, scale is perceived as an essential component, needed to make the concept of reputation work (Dellarocas 2003). Second, but tightly linked, is the notion that reputation needs to be spread and shared to be beneficial (Castelfranchi and Falcone 1998; Mui et al. 2002a). Furthermore, it is interesting to note that the reputation of an agent is not absolute, but that the value can vary depending on the agent evaluating her (Mui et al. 2002b). Closely related is the ability of reputation to be both—uni- as well as bidirectional (Dellarocas 2000). This means that in an arbitrary transaction either only one side can rate the other or both can rate each other.

A property that is shared by both trust and reputation is context-dependence (see Section 2.1) (Mui et al. 2002b). However, this also holds true for the fact that some authors neglect this idea (Mui et al. 2002b) by only considering a single context.

The last commonality is the shared opinion that reputation typically makes use of a multitude of information sources. These tapped sources range from personal experience and witness/partner information (Kollock 1999; Mui et al. 2002b) up to non-verbal cues like facial expressions (Dellarocas 2003). While a given system could restrict itself to one potential information resource, Kollock (1999) implicitly states that using multiple ones usually is considered to be better than a single source.

2.4 Computational Reputation—Definition and Contrast to the Traditional Reputation Concept

As in the case of trust, there are computational reputation models that represent an extension of the reputation concept to the computational domain. Zacharia et al. (1999) proposed a separation into computational and non-computational models about 20 years ago.

While the classical form of reputation is an ancient and commonly used tool within human societies, computational reputation became one of the best governance tools (Yan et al. 2015) available on the Internet and thus is even characterized as one of the pillars of online marketplaces (Dellarocas 2003)—even despite its relatively short lifetime.

A classic example of such a reputation system (*and its success*) is the feedback mechanism used by eBay, which with a Gross Merchandise Volume of $81.7 billion is one of the largest global online marketplaces (eBay Inc. 2015). Additionally, the use of IT allows some degree of control and monitoring of past transactions, which is impossible for a human agent (Dellarocas 2003). While a human may be able to remember past interactions, an Information Systems (IS) can precisely measure outcomes of previous interactions and store the results without a gap. Another advantage lies within the low costs that are associated with the collection and distribution of reputation information on the web (Kollock 1999). Kollock (1999) identified this beneficial cost structure as a key enabler for many currently existing online reputation systems.

However, computational reputation also comes at the cost of several new threats and disadvantages—which is one of the reasons why it is still an area of extensive research. First, among the drawbacks, is the feedback provision (*used to compute reputation scores*). This provision is often - as in the case of eBay—voluntarily (Dellarocas 2003), so that selfish agents might neglect sharing their information (*or at least sharing it truthfully*) (Arenas et al. 2010) and thus work against the essential building blocks of scale and information sharing (*see the previous section*). Insecurities also exist concerning the aggregation of collected information. The low point here is that no fixed model exists that prescribes the ideal degree of aggregation or the relevant time span (Dellarocas 2003).

Besides these inherent disadvantages within the system, there is also a set of actual threats and attacks to reputation systems that have surfaced in previous years. One of these is self-promotion (Hoffman et al. 2009) or ballot stuffing (Dellarocas 2000), both aiming at increasing one's reputation, via manipulation. Another is the opposite strategy of slandering (Hoffman et al. 2009) or bad-mouthing (Dellarocas 2000), where an agent/a group of agents tries to lower opponent agents reputation score by false ratings. Even more critical, and especially facilitated by computational reputation models, are the cheap pseudonyms (for examples of such behavior, refer to Friedman and Resnick (2001)). These allow malicious agents to build up a reputation only for cheating other agents, escaping potential consequences by taking up a new identity/pseudonym at nearly no cost (Hoffman et al. 2009).

To further exploit advantages while fixing existing issues, computational reputation (models) have been researched over the past years and are still an active branch of research as the review in Section 4 shows.

In conclusion for this section, a hint mentioned by Jøsang et al. (2007) shall be put forward. They claim that there is some risk in mixing up Reputation System (RS) and Collaborative Filtering (CF) systems, as both are collecting user ratings. Jøsang et al. (2007), however, try to make clear that both systems are in fact quite distinct. To make their point, they explain that CF was much more optimistic in searching for the ideal choice, while RS was pessimistic, trying to eliminate the worst choice. Additionally, they claim that RS allows agents to defect, whereas the same is not possible for CF. While at this point the distinct characteristics should be relatively clear, it has to be mentioned that none of the top-cited papers (based on the citations counted by the Google Scholar index) regarding "*collaborative filtering*" even contained the word "*reputation*" (Breese et al. 1998; Herlocker et al. 2004; Linden et al. 2003; Resnick et al. 1994; Sarwar et al. 2001). This, while good for learning the semantic differences, also evidentiates the overall chance to interchange the terms.

2.5 Defining the Relation of (Computational) Reputation and Trust

When reading through the existing literature related to the topic of "*Computational Trust and Reputation models*," one may recognize that it is hard to understand the differences between reputation and trust. This problem was already observed back in 2002 by Mui et al. (2002a, 2002b), who also complained about the confusion around these two terms.

However, taking a closer look in the literature again does not help in resolving the issue. The only idea that most publications of EBSCO share is that both concepts are in a close relationship (Abdul-Rahman and Hailes 2000; Dellarocas 2003; Lu et al. 2009). All unity is gone when looking at "how" the relationships are supposed to look. For example, there exists a fairly large group of authors that perceive reputation as a significant input or contributing factor to the trust computation (see, e.g., Abdul-Rahman and Hailes (2000), Dellarocas (2003), Kravari and Bassiliades (2016), Pinyol and Sabater-Mir (2013b), and Ruohomaa et al. (2007)). Others like Zacharia et al. (1999), however, understand reputation as the amount of trust a certain agent is able to generate in a particular domain. Authors like Lu et al. (2009), for whom reputation is just non-private/socialized trust (*every form of trust not kept private at a given agent*). A last, major group identified during the preparation of this survey compromises the proponents of leaving trust, reputation, and their relationship undefined (Yu et al. 2013).

3 RESEARCH METHODOLOGY

3.1 Selection of Papers

This systematic review was conducted according to the protocol presented by Kitchenham and Charters (2007) to increase the reproducibility of the conducted research. Five leading databases in the area of academic research were used to conduct the search (i.e., EBSCOHost, ACM Digital Library, SCOPUS, Science Direct, and Web of Science). These bases were selected due to their broad coverage and to the fact that they have relevant works regarding the topic examined in this review.

Moreover, the approach also follows the recommendations of Webster and Watson (2002) to go beyond the core discipline of IS and look at related disciplines. The main objective of this study is to identify the current state of research into the use of Computational Trust and Reputation models,[1] the following search terms were used: "*computational trust*" and "*reputation model.*" In conformity with recommendations for initial research synthesis (Cooper et al. 2009), the keywords selected were sufficiently broad to avoid limiting results and still provided restrictions to prevent undesirable results. Here it has to be noted that the quotation marks were intentionally used, to force the search engine to only select papers using the exact word sequence. This avoids selecting papers dealing with "*trust*" and "*computational*" but not "*computational trust.*" To fulfill the aim of categorizing only recent approaches, the selection was restricted to the span of 2013–2016, so that only the past three years, coinciding with the yet uncovered period of 2013 until today.[2]

As further restrictions, only journal articles were considered, excluding book chapters, dissertations, and conference proceedings. This is based on the idea that journals are typically deemed to provide the maximum amount of scientific rigor and have the greatest academic impact (see (Freyne et al. 2010; Vardi 2009)). Furthermore, each paper should provide an implementation or at least a simulation/experiment that indicates that the approach has been implemented at least once. By doing so, we are ensured that the proposed systems can be implemented and, based on the

[1] The term *model* is used as an umbrella term for all analyzed contributions. While some are presented as an actual implementation, the focus of this article is the underlying theoretical trust and/or reputation concept. The restriction to the term model has been made in a strong belief that it underlines the article's focus and avoids confusion caused by ambiguous terminology.

[2] Considering the last mentioned survey paper by Pinyol and Sabater-Mir (2013b). At least one other survey paper is known, which, however, focuses on different aspects (Bidgoly and Ladani 2015). So, to the best of our knowledge, this survey paper provides novel research.

Table 2. General Paper Characteristics

Short	Characteristic	Meaning
Lib	Bibliography Entry	the bibliography entry of the paper being its UID throughout this article
Jou	Journal	the journal in which the paper was published
Cit	Citation Count	citations counted for the respective paper by Google Scholar
ACi	Adjusted Citation Count	citation count averaged over the past years (base is 2016 = 1, 2015 = 2, . . .)
ApA	Application Area	the application area considered for the model proposed in the paper

published tests, their rough performance can be estimated. Additional general exclusion criteria were not considered. If special reasons made it necessary to leave out a paper, then the reasons were noted separately (see those in Online Appendix B).

3.2 Criteria for Comparison

After obtaining a representative selection of papers (i.e., a total of 189 studies were returned in the *Collection phase*), the next logical step for this article was to analyze and compare the found articles using a predefined schema. For this purpose, this article follows the proposal of Webster and Watson (2002), to use so-called concept matrices to compare different articles on the basis of a fixed set of concepts. Using this approach is in line with previous reviews (Lu et al. 2009; Pinyol and Sabater-Mir 2013b; Ruohomaa et al. 2007) that form the foundation for this article, as they also make extensive use of matrices to achieve a clear presentation of their results.

Since previous studies provide a lot of insightful concepts and characteristics, which can be used to compare computational trust and reputation models, the decision was made to divide the matrix into four matrices. The first matrix (used criteria see Table 2) is used to give general information regarding each paper. For example, the citation count according to Google Scholar is given as an indicator of the academic importance of an article (Thomson Reuters 2014). To account for the fact that more recent publications might have fewer citations, an averaged count is given to make comparison easier.[3]

The second matrix (for utilized criteria, refer to Table 3) provides deeper insights into the actual models. It is almost completely derived from the publications of Pinyol and Sabater-Mir (2013b), Sabater and Sierra (2005), and Balke et al. (2009). These review papers already provide an extensive review scheme that has been successfully applied to computational trust and reputation model research. Reusing their approach creates a consistent stream of research that provides readers with the ability to compare models among papers.

For more detailed explanations of individual characteristics, a closer look at the original research papers is recommended. The only notable addition is that especially for *Par*, *InS* and *Vis* (see Table 3) some papers only provided implicit information, so that estimations had to be made (*or N/A had to be used, in cases where insufficient data was identified*).

Among all matrices, the third (Table 4, referring to used criteria) has the special property of being a completely Boolean matrix. It only contains characteristics/concepts that can be sufficiently answered by TRUE/FALSE. The concepts *Dec*, *Cog*, *Pro*, *Gen*, and *ReM*, are characteristics derived from the Pinyol and Sabater-Mir (2013b) paper, where they added these as additions to the ones already defined by Sabater and Sierra (2005) and Balke et al. (2009). While again all additional information

[3] That the measure at this point may be statistically flawed has to be acknowledged. However, it should provide an intuitive idea whether a paper on average has been more or less widespread throughout the academic community.

Table 3. Characteristics used for Basic Comparison

Short	**Characteristic**	**Meaning**
Type	Type/Recall of Cooperative Behavior	The type characteristic informs about whether each agent only considers agent-internal information (*denoted as trust information*) or whether it also integrates external information from the overarching system or other agents as well (*denoted as reputation*).
Par	Paradigm/Conceptual Model	The paradigm indicates whether trust/reputation is understood as either cognitive (*built on beliefs/mental states of an agent*) or numerical (*e.g., game theoretical approaches lacking cognitive attitudes*).
InS	Information Source	Refers to the tapped information sources (*reaching from direct experiences of an agent to witness information or prejudice*)—multiple sources can be used.
Vis	Visibility/Storage	Visibility specifies the type of trust/reputation storage—typically, either a global property that can be read and adjusted by each agent or a private property of each only accessible to the agent itself.
Gra	Model's Granularity	The granularity defines whether the model considers only a single context (*one trust/reputation value per agent*) or multiple contexts (*multiple trust/reputation values per agent each with regard to another context/property*).
Che	Cheating Behavior	Defines to which extent cheating behavior is considered (*from not at all up to the provision of specific mechanisms to deal with lies*).
ExI	Type of Exchanged Information	Specifies the (data) type of exchanged information typically being either Boolean or continuous.

Based on: Balke et al. (2009), Pinyol and Sabater-Mir (2013b), and Sabater and Sierra (2005).

can be derived from the original paper, it has to be noted that the *Dec* and *ReM* classifications are off-spins of Pinyol and Sabater-Mir (2013b) trust classification.

The categories *CTN* and *RiM* are derived from the paper by Lu et al. (2009), whereas *CoL* is a measure originally defined by Yu et al. (2013). Apart from these inferred characteristics, a couple of categories were added: The first is *Ref*, which has been added to have the ability to distinguish between newly proposed models and reference models providing best practices derived from already existing approaches (Becker et al. 2008; Rosemann and van der Aalst 2007). A second add-on is the MAS characteristic, which accounts for the often mentioned tight link between computational trust and reputation models and *MAS* (Marsh 1994; Yu et al. 2013). The last additional metric is the *Tem* aspect, which should help to evaluate whether a model considers temporal aspects. It follows the intuitive logic of authors like Jøsang and Ismail (2002) and Marsh (1994), who point out that agent behaviors are dynamic and may change over time so that more recent actions might deserve more weight.

Table 4. Boolean Characteristics

Short	Characteristic	Meaning
Dec	Decision	determines whether a given model provides a concept to determine the cooperation partner based on trust/reputation
Cog	Cognitive	the paper provides reasoning on WHY certain steps are taken
Pro	Procedural	the paper provides an explanation on HOW certain steps have to be taken
Gen	Generality	indicates whether a model is rather general purpose or not
Ref	Reference/Maturity model	marks whether a model can be considered as a reference/maturity model
MAS	Use of MAS	indicates whether a model makes use of MAS
Tem	Temporal Aspects	is time considered as an influence factor on trust/reputation values
CTN	Consideration Trust Network	determine whether a model details the topology of a trust network for information propagation
RiM	Risk Management	the paper provides an approach to handle the model risk (*environmental risk*)
ReM	Reliability Measure	the paper provides an indication of the model's reliability
CoL	Computational Limits	the model considers potential computational limits (*CPU, storage, . . .*)

Based on: Lu et al. (2009), Pinyol and Sabater-Mir (2013b), and Yu et al. (2013).

Table 5. Characteristics used for Additional Comparison

Short	Characteristic	Meaning
Def	Definitions	how does the paper define trust/reputation and the developed models (*textual, logical, mathematical*)?
NuP	Number of Peers	how many peers are considered when information is aggregated (*scalability vs. representation*)
Agg	Aggregation	by which means are the trust/reputation values aggregated; which mathematical functions are used
Sel	Selection of Partners	how are the cooperation partners selected based on the aggregated values
Act	Proposed Actors	which kind of potential actors does the model/it's simulation consider
Eva	Evaluation Data	how is the proposed model evaluated and which kind of data is used

Based on: Lu et al. (2009), Ruohomaa et al. (2007), and Yu et al. (2013).

The fourth and last matrix (Table 5, referring to used criteria) provides additional information that did not fit into the previous ones. One large difference is the fact that this matrix contains mainly characteristics/concepts requiring free answers, since they are hard to put into confined categories. Notable exceptions are the *Def* characteristic proposed by Lu et al. (2009), as well as *Eva* taken from Yu et al. (2013) and *Act* originating in Ruohomaa et al. (2007). Of these measures *Eva* is especially interesting, as depending on the data used for evaluation, a cross-model comparison is possible or not possible (*synthetic, simulated data makes it difficult, whereas standardized test* *datasets are beneficial*). The remaining concepts have all been originally proposed by Ruohomaa et al. (2007) and allow additional insights into the model quality. For example, the methods used for *Agg* and *Sel* can have considerable influence on the results, as *NuP* can be a major determinant for the quality of the accumulated (witness) data.

4 RESULTS AND ANALYSIS

With the search parameters defined in Section 3.1, 189 papers were discovered, of which 40 have been accepted for this review (see Table 6), while 72 papers were rejected (see Table 13) and 77 papers are duplicates of the accepted or rejected publications. In terms of pure results, the Web of Science has been the most resourceful; however, EBSCOHost has been found to deliver more relevant papers for this survey—directly followed by the Web of Science (see Figures 2(a) and 2(b)). The other three search engines delivered only about 25% of all results. The exact numbers of accepts, rejects and duplications are visualized in Figure 3. There it should be noted that for example the high number of duplicates for the Web of Science could be the result of the review order in which it was considered last.

Looking at the results that have been discovered and selected for this review (see Table 6), it becomes apparent that the presented models have been developed in various areas of academia. These range from business related topics, like e-commerce (Majd and Balakrishnan 2015; Ransi and Kobti 2014) and supply chains (Chang et al. 2014), over wireless communication systems (Lin et al. 2015; Wang et al. 2016) to general approaches not explicitly aimed at a certain domain (Ashtiani and Azgomi 2014; Yu et al. 2014a). As a consequence, the source journals are also representatives of various research areas.

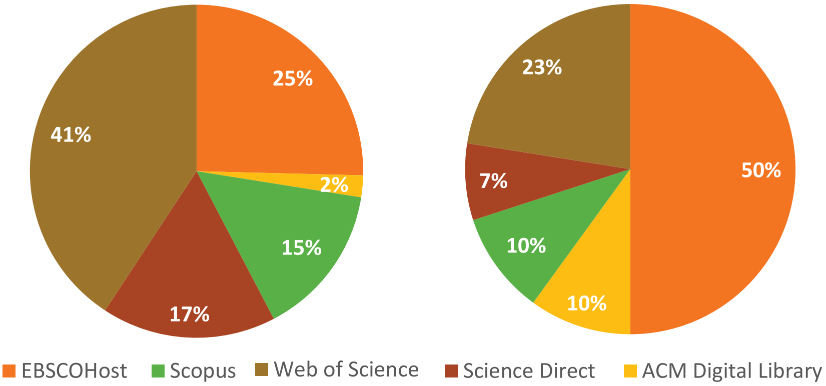
Regarding citations, it can be stated that most papers thus far have received very few citations. Two papers have yet to receive a single citation, and only 12 have citation-rates greater than 10. However, it appears to be flawed to compare citation counts of papers from 2013 with those published in 2016. To obtain a better metric to compare the counts the factor of time has to be eliminated. This is achieved by computing the average citation count (ACi) over time for each publication. The metric is computed by dividing the citations of the given publication by the duration in years that it is available (so, e.g., by one for the year 2016 and by two for the year 2015). Analyzed with this new metric the range decreases from 0–37 to 0–15, indicating that the majority of trust and reputation related publications in the last three years received approximately similar attention. The papers with outstanding citation counts are surprisingly among the newest publications (e.g., Acampora et al. (2016), Messina et al. (2016), and Yan et al. (2015), with ACi 15, 14, 13, respectively) instead of those from 2013. Considering only the citation count, the paper of Lee et al. (2013) (Cit: 37) would have received a better score when compared with the publication of Acampora et al. (2016) (Cit: 15); this situation is reverted when using the ACi metric, where the papers obtained the score of 9.25 and 15, respectively.

The general paper characteristics (see Table 7[4]) provide additional insights regarding the contents of the papers. It can be learned that most presented models and mechanisms are not purebred but contain associations to both trust and reputation. A common notion in such papers is the use of reputation to establish trust (Ashtiani and Azgomi 2014), which can be found in different formulations and degrees of interconnection. Considering the used *Information Sources*, one can observe that most models (26 out of 40 (65%)) use multiple sources, with only 11 models being restricted to a single source (27.5%). At this point, it can be added that most multi-source models consider witness and direct information, whereas prejudice and sociological information are only used in rare cases. Similarly unbalanced are the characteristics of *Visibility* and *Granularity*, which indicate a

[4] Tables with shortcuts of the characteristic values can be found in Appendix A in Tables 11 and 12.

Table 6. Analyzed Papers Including Publication Information

	Lib	Journal	Cit	ACi	ApA
1	Ashtiani and Azgomi (2014)	Advances in Complex Systems	4	1.33	General
2	Liu et al. (2013)	Electronic Commerce Research and Applications	31	7.75	General
3	Wierzbicki et al. (2013)	Decision Support Systems	10	2.5	Internet Auctions
4	Trček (2014)	Informatica	2	0.66	General
5	Urbano et al. (2014)	AI Communications	5	1.66	General
6	Hammer et al. (2015)	User Modeling and User-Adapted Interaction	16	8	Smart devices
7	Majd and Balakrishnan (2015)	Journal of Intelligent & Fuzzy Systems	0	0	E-Commerce
8	Lee et al. (2013)	Frontiers in Psychology	37	9.25	HRI
9	Kravari and Bassiliades (2016)	The Journal of Systems and Software	3	3	General
10	Yan et al. (2015)	Information Sciences	26	13	E-Commerce
11	Ransi and Kobti (2014)	Axioms	3	0.75	E-Commerce
12	Kussul et al. (2013)	Computers & Security	18	4.5	Grid Systems
13	Yu et al. (2014a)	Sensors	11	3.66	Sensor Systems
14	Abdel-Hafez et al. (2015)	Web Intelligence	7	3.5	E-Commerce
15	Wei and Wang (2014)	New Generation Computing	0	0	Self-Organized Networks (SON)
16	Chang et al. (2014)	International Journal of Production Economics	24	8	Supply Chains
17	Tormo et al. (2015)	Future Generation Computer Systems	8	4	Internet of Things (IoT)
18	Wang et al. (2016)	International Journal of Distributed Sensor Networks	9	9	Vehicular Ad Hoc Network (VANET)
19	Lin et al. (2015)	International Journal of Distributed Sensor Networks	5	2.5	Cognitive Radio Networks
20	Giacomini and Agarwal (2013)	EURASIP Journal on Wireless Communications and Networking	8	2	Wireless Networks
21	Wang et al. (2013)	The Journal of Supercomputing	9	2.25	P2P-Voice over IP (VoIP)
22	Wu et al. (2015)	Enterprise Information Systems	5	2.5	Service-Oriented Computing (SOC)
23	Chandran et al. (2016)	The International Arab Journal of Information Technology	6	6	Cloud Computing
24	Ashtiani and Azgomi (2016b)	Applied Soft Computing	8	8	General
25	Acampora et al. (2016)	Information Sciences	15	15	P2P e-Commerce
26	Yu et al. (2014c)	Decision Support Systems	26	8.67	decision support online reviews
27	Pérez et al. (2014)	Journal of Computer and System Sciences	10	3.33	collaborative alert systems
28	Škorić et al. (2016)	International Journal of Information Security	4	4	Network security
29	Qureshi et al. (2013)	Multimedia tools and applications	7	1.75	MANET
30	Nguyen and Tran (2013)	International Journal of Innovative Computing, Information and Control	21	5.25	E-Commerce
31	Ashtiani and Azgomi (2016a)	Information Systems Frontiers	1	1	General
32	Lu et al. (2016)	Peer-to-Peer Networking and Applications	10	10	P2P file-sharing
33	Messina et al. (2016)	Future Generation Computer Systems	14	14	Cloud/Grid
34	Han et al. (2015)	Peer-to-Peer Networking and Applications	6	3	P2P networks
35	Li et al. (2015)	Knowledge and Information Systems	16	8	rating
36	Zhong et al. (2015)	IEEE Transactions on Dependable and Secure Computing	16	8	General
37	Jelenc and Trček (2014)	Autonomous Agents and Multi-Agent Systems	5	1.67	General
38	Bahtiyar and Çağlayan (2014)	Electronic Commerce Research and Applications	18	6	security for e-health
39	Kussul et al. (2015)	Computing and Informatics	1	0.5	Grid resource mgmt.
40	Tuna et al. (2013)	Elektronika ir Elektrotechnika	1	0.25	RSNs



(a) Distribution of All Results.

(b) Distribution of Accepted Results.

Fig. 2. Distribution of results across search engines.

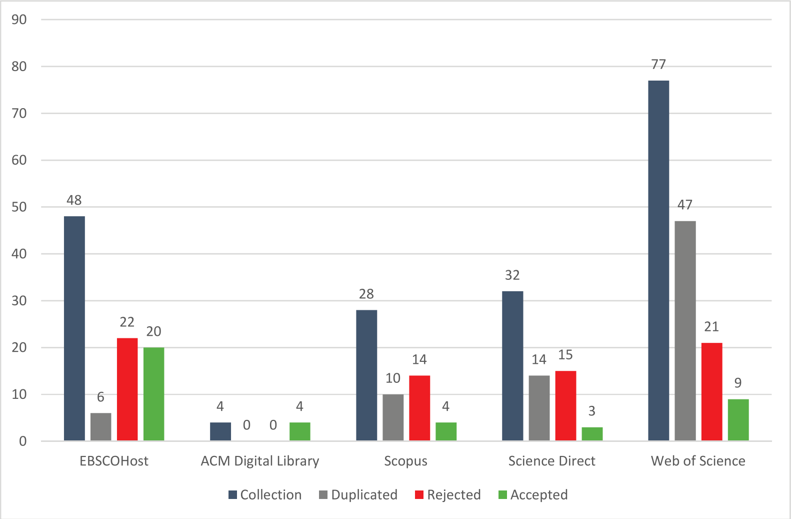


Fig. 3. Accepts, rejects, and duplicates per search engine.

preference for distributed multi-context models. This kind of distribution also applies to the last column, the *Type of Exchanged Information*, as most approaches deal with continuous data, while other formats like Booleans or value tuples are quite uncommon. Another notable aspect observed is *Cheating Behavior* as it is the only single-valued column. All models either consider cheating in Level 2[5] (Pinyol and Sabater-Mir 2013b) or do not deal with cheating behavior at all.

Concerning the Boolean characteristics presented in Table 8,[4] the most unambiguous column is regarding the *Reference Models*. In fact, none of the 40 analyzed trust and reputation models have been constructed as a reference model. The only column nearly that clear, but with positive instead of negative outcomes, is the *Procedural* column, since every analyzed paper at least partly explains the used process of trust and reputation computation. However, this only *partly* applies

[5] The Level 2 represents cheating behavior, while Level 1 would refer to keep things secret without lying and Level 0 to not considering cheating at all. For more information on the single levels, please refer to Pinyol and Sabater-Mir (2013b).

Table 7. General Paper Characteristics Result

	Type	Par	Ins	Vis	Gra	Che	ExI
1	T+R	Co	DI+WI	D	MC	L2	C
2	T	Nu	DI+WI+P	D	MC	L2	B+C
3	T+R	Nu	WI	N/A	MC	L2	C
4	T	Nu	WI	D	N/A	N/A	VM+V
5	T	Co	DI+WI+SI	D	MC	L2	C
6	T	Co	WI+SI	D	MC	N/A	N/A
7	T+R	Co	DI+WI	D	MC	L2	C
8	T	Co	DI+WI+SI	CT	SC	N/A	I+CC
9	T+R	Co	DI+WI+SI	D	MC	L2	B+C
10	T+R	Co	DI+WI+SI	D	MC	L2	C
11	T+R	Nu	DI+WI	CT	MC	N/A	C
12	T+R	Nu	DI	CT	MC	L2	C
13	R	Nu	DI	CT+D	SC	L2	C
14	R	Nu	N/A	N/A	SC	N/A	N/A
15	R	Nu	DI+WI	D	SC	L2	C
16	T+R	Nu	DI+WI	D	MC	L2	C
17	T+R	V	DI+WI	CT+D	N/A	L2	C
18	T+R	Nu	DI+WI	CT	SC	L2	T[a]
19	T+R	Co	DI	D	S/MC	L2	C
20	R	Nu	DI+WI	D	SC	N/A	C+B
21	R	Nu	WI	D	MC	L2	T[b]
22	R	Co	DI+WI	CT	S/MC	L2	T[c]
23	T+R	Nu	DI+WI	D	SC	N/A	C
24	T+R	Co	DI+WI+SI	D	MC	L2	VM+FS
25	T+R	Co	DI+WI	D	MC	L2	C
26	T+R	Nu	DI+WI	D	SC	L2	B
27	T+R	Nu	WI	D	SC	N/A	A+C
28	R	Co	DI+WI	D	SC	N/A	C
29	T+R	Nu	DI+WI	D	SC	L2	B
30	T+R	Nu	DI+WI	D	SC	N/A	C
31	T	Co	DI+WI	D	MC	L2	C
32	R	Nu	DI	D	SC	N/A	B+C
33	T	Nu	DI+WI	D	SC	~	B+C
34	T	Nu	WI	D/CT	SC	N/A	C
35	R	Nu	WI	D	SC	N/A	C
36	T+R	Nu	DI	CT	SC+MC	N/A	B
37	T	Co	DI+WI	D	MC	L2	CC
38	T	Nu	DI+WI	D	SC	N/A	C
39	R	Nu	N/A	D	SC	N/A	C
40	T+R	Nu	DI+WI	D	SC	L2	I

[a] tuple: {keys, certificates, messages}.

[b] tuple containing keys and continuous values.

[c] 4-tuple: {belief, disbelief, uncertainty, a priori belief}.

Table 8. Boolean Paper Characteristics Result

	Dec	Cog	Pro	Gen	Ref	MAS	Tem	CTN	RiM	ReM	CoL
1	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓	✗
2	✓	✓	✓	✓	✗	✓	✗	~	✗	✗	✗
3	~	✓	✓	✗	✗	N/A	✗	✗	✗	✗	✗
4	~	✓	~	✓	✗	~	✗	✗	✗	✗	✗
5	✓	✓	✓	✓	✗	~	✓	✗	✗	✗	✗
6	✓	✗	~	~	✗	✗	~	✗	✗	✗	✗
7	✓	✓	✓	✗	✗	✓	✓	✓[a]	✓	✓	✗
8	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗
9	✗	✓	✓	✓	✗	✓	~	✓	✗	✓[b]	✓
10	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓[b]	✗
11	✗	✗	~	✓	✗	✓	✗	✗	✗	✗	✗
12	~	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
13	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
14	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
15	~	✓	✓	~	✗	✗	✗	✗	✗	✓	✗
16	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗
17	✓	✓	✓	✓	✗	✗	~	✗	✗	✗	✓
18	✗	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
19	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
20	✓	~	~	✗	✗	✗	✓	✗	✗	✗	✓
21	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗
22	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗
23	~	~	~	✗	✗	✗	✓	✗	✗	✗	✗
24	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗
25	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗
26	✓	✗	✓	✓	✗	✓	✗	✗	✗	✓	✗
27	✗	✗	✓	✓	✗	✗	✓	✗	✓	✓	✓
28	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗
29	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗
30	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✓
31	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗
32	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗
33	✓	✓	✓	✗	✗	✓	~	✓	✗	✗	✗
34	✗	✓	✓	✗	✗	✗	~	✓	✗	✗	✗
35	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
36	✓	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗
37	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✗
38	✓	✗	✓	✗	✗	✗	✓	✗	✓	✓	✗
39	✗	✗	~	✗	✗	✗	✓	✗	✗	✗	✗
40	✗	✓	✓	✗	✗	✗	✗	✓	✗	✓	~

[a] In the paper, there is no explicit definition of a trust network. However, it breaks down the set of potential advisors into a small set by introducing explicit requirements, such as having interacted with a target before and reaching a certain reputation. Since this comes close to what is considered a trust network, the TRUE valuation was chosen.

[b] Values that could be considered to be reliability measures are used—yet not in that function and not with that label.

to 6 out of 40 papers, with the remaining 34 providing a procedural overview to the reader. The *Cognitive* aspect is not so straightforward, as at least ten papers do not provide any reasoning on why certain steps have been taken. Even fewer (11 out of 40 (27.5%)) provide insights on how exactly they finally select their interaction partner. The evaluation of the *Generality* and *Temporal Aspects* characteristics leads to similar observations of more or less mixed results.

Regarding the characteristics, *Use of MAS*, *Consideration Trust Networks*, *Risk Management*, *Reliability Measures*, and *Computational Limits* the TRUE evaluations start to digress. In values, this resolves to only five models acknowledging the existence of computational limits and risk management, whereas at least 11 papers consider the usage of reliability measures. The *Use of MAS* with 10 TRUE and two "*partly*" valuations is already at the upper border of the rather unrecognized characteristics.

While the previous three tables provided a lot of shared values that allowed us to draw comparisons, the table regarding additional characteristics (Table 9[4]) contains a lot of unique, free-text entries. One of the comparable characteristics is *Definitions*. The majority (38 out of 40 (95%)) of the papers define their concepts providing both, a textual description of their steps as well as the *formulae* necessary to compute the presented values. Only two neglect to present the math used to build up the method and the in particular the subsequent simulation, i.e., Hammer et al. (2015) and Lee et al. (2013). Regarding the *Number of Peers Considered* the degree of clarity reduces, as about half of the papers do not provide any details. Among the others, a tendency can be found that indicates that most subsets of all potentially available peers are concerned for interaction. The situation is similar for the *Proposed Actors*, where 12 out of 40 papers do not offer any insights. Those who do typically use agents (23 out of 28 cases (82%)). The last column providing a lot of similar data is the one regarding *Evaluation Method/Data*.

In the columns regarding *Aggregation* (Agg) and *Selection of Partners* (Sel), mostly unique approaches (or N/A) are listed. Especially concerning partner selection, many rows are empty, as not every model includes this step (see Table 8). Of the selected papers, most make use of threshold or rank based selection. However other approaches like Pareto optimality, Support Vector Machine (SVM) classification, or degree of membership in a group are also implemented. Even more variation is provided in the *Aggregation* column. While weighted sums and means are often used, they do not dominate the characteristic. Various aggregation mechanisms reaching from Artificial Neural Network (ANN), Beta distribution, ID3 algorithm over defeasible logic up to SVMs are present in the analyzed models, making this column the least standardized among all columns used for evaluation (of content).

5 DESCRIPTION OF REVIEWED MODELS

The following section provides a short summary of each reviewed paper to outline its central idea as well as the basics of the presented trust/reputation models. To structure the descriptions, the papers have been grouped by their type/recall of cooperative behavior (see Tables 3 and 7), so that first all ten *trust* papers are presented, followed by eleven *reputation* and nineteen *hybrid* papers (cf. Figure 4).

5.1 Trust Models

5.1.1 StereoTrust. The *StereoTrust* model has been proposed by Liu et al. (2013) (ID 2 in Table 6) to handle new agents (*trust toward them*), for whom no historical interaction information is available. The inspiration for this model has been taken from the use of stereotypes in real life (*trying*

Table 9. Additional Paper Characteristics Result

	Def	NuP	Agg	Sel	Act	Eva
1	T+M	S	WS+QP+BI	TH/R	Ag	SD
2	T+M	S	BDist+WS	Gr	Ag	StdD+SD
3	T+M	N/A	WS/AVG+EDist	PO+R	N/A	SD
4	T+M	A	value matrices	N	Ag	SD
5	T+M	N/A	domain restricted sine function+Regr and Classif+ID3	R	Ag	SD
6	T	N/A	N/A	R	D+H	LSt+LS
7	T+M	S	(1) S/SIM between two V; (2) CFS	1) TH | 2) R	Ag	SD
8	T	N/A	select features from human study and train SVM and HMM	SVM+HMM	SVM+HMM	St
9	T+L	S	DL+WS	N/A	Ag	StdD
10	T+M	S	CFS (weighted reputation values)	N/A	Ag	SD
11	T+M	S	WM	N/A	Ag	SD+WD
12	T+M	S	SM (+ ANN for transformation)	PO+R	N/A	WD+SD
13	T+M	A	TM (+ sigmoid/Gompertz function)	N/A	N/A	SD
14	T+M	N/A	WAVG+NDist+DirMet	N/A	N/A	StdD
15	T+M	S	negative MDist+DirDist+smoothing	TH	N/A	SD[a]
16	T+M	A/S	WM	R	Ag	SD[a]
17	T+M	N/A	varying	varying	N/A	SD
18	T+M	N/A	WS (+ entropy)+WS (+ majority rule)	N/A	V	SD+RWM
19	T+M	N/A	WS	R	N/A	SD[a]
20	T+M	N/A	WS	TH	N/A	SD[a]
21	T+M	S	WP	TH	N/A	SD
22	T+M	S	WS + BDist/DirDist + ANN	N/A	N/A	SD
23	T+M	N/A	WAVG+NN+FL	TH	H	StdD[b]
24	T+M	A[c]	LAO+WAVG	NDD+R	Ag	SD
25	T+M	S	IT2FLS+WAVG	TH	H+Ag	WD+SD
26	T+M	S	WS + S/SIM + RL	R+TH	Ag	SD
27	T+M	S	WS / WM	TH	Ag	SD
28	T+M+L	S	SL/EBSL	TH	Ag	StdD+SD
29	T+M	S	WS	TH	Ag	SD
30	T+M	S	WS + AVG	N/A	Ag	SD
31	T+M	S	QP + QDT	R	Ag	SD
32	T+M	S	WS + Classif	N/A	H/Ag	SD
33	T+M	S	WS	N	Ag	SD
34	T+M	S	WS	R+TH	Ag	SD
35	T+M	S	WS+WAVG	N/A	H	SD+LS
36	T+M	S	DES	TH	N/A	SD
37	T+M	A	Distribution Vector	R+TH	Ag	StdD+SD
38	T+M	S	WS	N/A	Ag	SD
39	T+M	A	WS + CSF	PO+TH	Ag	SD
40	T+M	A	WS	R	N/A	SD

[a] The use of simulation data is not explicitly mentioned in the paper. However, the execution of simulations without the origin of the dataset being mentioned, allows the assumption that simulation data is used.

[b] The authors are explicitly mentioning the usage of (given) data sets leading to the assumption that most likely some (unnamed) standardized data sets have been used.

[c] All peers are considered, but through a waiting schema only a subset will have a substantial impact.

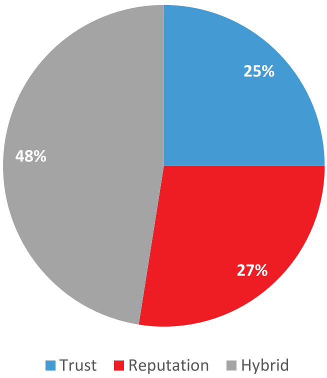


Fig. 4. Distribution of type/recall of cooperative behavior.

to derive values from knowledge of interaction with similar people). In a computational equivalent, this would map to the matching of the judging agents' stereotypes with profiles of other agents.

The used algorithm starts with similar grouping agents into separate groups, where each group is a fuzzy set of agents. The model computes the trust between groups the current agent and the created groups making use of beta distribution to model uncertainty. Deriving the trust value of the target agent is done by creating the weighted sum of the current agent's trust into groups the trustee is also a member of.

As Liu et al. (2013) had to acknowledge that their model has some downsides, they proposed two extensions: The first one called *d-StereoTrust* further subdivides the created groups into subgroups of honest and dishonest agents to improve prediction quality. A second one, which they call Stereotypes Sharing Overlay Network (SSON), aims at sharing stereotypes between agents to support yet inexperienced trustors.

5.1.2 Qualitative Assessment Dynamics. Similar to Wierzbicki et al. (2013), Trček (2014) (ID 4 in Table 6) also proposes an add-on method to complement already existing systems. He explicitly points out that he expects no single method to be successful but rather prefers a multi-method system.

To improve the handling of dynamic trust in e-environments, Trček (2014) proposes Qualitative Assessment Dynamics (QAD) being both a formal system as well as a simulation framework. The depicted specialty of QAD is supposed to be a human-agent focused methodology. It is implemented to consider human deficiencies like irrationality, lack of understanding of complex math, lack of preferences concerning trust, and so on.

5.1.3 Sinalpha + Social Tuner + Contextual Fitness. Urbano et al. (2014) (ID 5 in Table 6) figured out that existing models were not using social ideas like the relationship under which a transaction is conducted (also called *semantic of evidence*).

As a first step, they create eleven guiding propositions based on the insights on social trust that they generated. Driven by their guidelines, Urbano et al. (2014) propose a system consisting of three separate components: The first they called *Sinalpha*. It computes an α value that expresses the trusting behavior. Afterward, it uses the α value to compute a first trustworthiness value tw_{sin}, which is a monotonic aggregation function with a sinusoidal shape.

The second component—and one of the major contributions—is the so-called *Social Tuner*. It takes the previously calculated tw_{sin} as an input and aims at adjusting the value based on a cognitive/emotional component.

As a third component and second proposal a *Contextual Fitness Filter* is presented. Based on the values found by an ID3 classification algorithm a fitness score for the given context is computed and again used to weight the trustworthiness score. To test their new approach—and to present a standard testbed—Urbano et al. (2014) also present a new evaluation model based on their eleven propositions. It allows for the evaluation of methods for more complex agents, which can consider elements such as *effort, ability, benevolence*, among others.

5.1.4 User Trust Model. Deviating from many of the other presented approaches, Hammer et al. (2015) (ID 6 in Table 6) do not propose a model that is meant to handle trust between two artificial agents. Instead, they present the User Trust Model (UTM) that should allow artificial systems to evaluate whether a certain action would be perceived as trustworthy. The suggested areas of application are pervasive systems like home or office automation systems, yet it is supposed to be adjustable to other domains as well. In these pervasive/smart systems (*or any other domain*), UTM should help to decide which actions are appropriate for a user (*e.g., light on or off*).

Based on survey data, Hammer et al. (2015) figured out that a set of trust dimensions exist and that have an influence on how trustworthy users evaluate systems. The set includes the *comfort of use, transparency, controllability, privacy, and security*, which share the characteristic of being hidden, non-directly observable variables. To model these dimensions, Bayesian networks were chosen.

Such a network can subsequently be trained and is then able to assign a utility value to different actions to decide on the degree of trustworthiness. Conducted experiments with small samples were deemed successful by Hammer et al. (2015), yet hinting that larger groups might provide even more meaningful results.

5.1.5 Lee et al. Similar to Hammer et al. (2015) the trust model suggested by Lee et al. (2013) (ID 8 in Table 6) does not consider (*digital*) agent-to-agent interaction. Instead, they focus on human-robot interaction by trying to develop a model that would allow robots to predict the amount of trust a potential partner has toward them.

In a first step, the authors carry out a study to obtain information/material regarding the non-verbal cues that they want to classify to predict the degree of trust and to generate the needed data. The data is used to create a SVM classification model. After the training phase, the SVM is able to classify new data items into one of the learned classes.

To further improve their model, Lee et al. (2013) introduced the Hidden Markov Model (HMM) to identify temporal patterns within their data. They admitted the limited analytical use (*black-box model*), yet pointed out that pattern information might enhance the given SVM classifier. With the raw data, the HMM model is trained to be able to simulate realistic behavioral paths. After numerical encoding, the authors successfully used the generated data to enhance the previously created SVM.

5.1.6 Computational Trust Based on Quantum Decision Theory. In their 2016 Information Systems Frontiers publication, Ashtiani and Azgomi (2016a) (ID 31 in Table 6) extend their earlier work (Ashtiani and Azgomi 2014) on computational trust based on quantum decision theory (QDT). One of their major arguments is the concept of superposition, which allows expressing fuzziness and ambivalence in a more natural yet more mathematically precise fashion, such as $|\Psi\rangle = \alpha_0|\text{distrust}\rangle + \alpha_1|\text{trust}\rangle$, where the trustor can trust and distrust at the same time. Also, their quantum vector model allows us to include different trustworthiness criteria, such as competence or motivation, to include both subjective and objective points of view as well as to accommodate different contexts.

5.1.7 *Hypertrust.*

Messina et al. (2016) (ID 33 in Table 6) propose a novel decentralized trust model for resource finding and allocation in large-scale, competitive computing environments. Similar to many of the other approaches, Hypertrust makes use of both direct experiences and second-hand information from peers to assess resources. To account for malicious peer behavior, Messina et al. (2016) include preference measures to give each feedback providing peer a weighting. The generated Hypertrust model is subsequently used by the authors to create an overlay network over the computing resources to enable trust-based resource allocation. Messina et al. (2016) conclude their paper by several simulation experiments, which they use to assess the suitability of their approach but also to tune the parameters of the Hypertrust model.

5.1.8 *Topological Potential Weighted Community-Based Recommendation Trust Model.*

With TPCommuTrust, Han et al. (2015) (ID 34 in Table 6) introduce a further trust model for P2P networks that integrates the concepts of a community (P2P subgroup with similar resources and interests), peer access control, and topological potential (weighting of the power of a node in a network). The actual trust score of an agent includes three components: First, a behavioral component is added to account for the behavior and contributions of an agent in a fixed time period. Second, and as a novel contribution according to Han et al. (2015), a community component is included to assess the behavior of a community, e.g., to prevent collaborative misbehavior. Third, reputation, respectively, recommendations, is added to avoid the cold start problem for novel agents. To account for the split of the P2P network into separate communities, Han et al. (2015) also propose two trust exchange mechanisms for communication within and across communities.

5.1.9 *Qualitative Trust Model.*

To provide a trust model that can work with and output human-readable and understandable trust values, Jelenc and Trček (2014) (ID 37 in Table 6) propose a novel model using qualitative and ordinal values. Hence, they position their model as a somewhat generic solution for situations where human interaction with a system is crucial. Similar to many of the other models, Jelenc and Trček (2014) use both directly obtained information as well as opinions of other agents to deduce a trust score. To appropriately deal with the qualitative or ordinal data handling and aggregation is performed by distribution vectors. Cheating and malicious behavior of opinion providing agents are encountered with the addition of credibility weightings taking into account opinion recency, the trustworthiness of opinion provider and potential social links.

5.1.10 *Trust Assessment of Security for e-Health Systems.*

Bahtiyar and Çağlayan (2014) (ID 38 in Table 6) introduce a novel trust assessment model for the domain of e-health systems that is intended to increase trust in digital healthcare services. They build this model upon the idea of a so-called trust assessment system, which they link to each entity—another concept under which they subsume devices or software used to access an e-health service. It collects, e.g., security policies, security mechanisms, and logs as provided by the healthcare service to assess its trustworthiness, also considering observed behavioral information as well as observations of other entities. From this information, six trust metrics are computed that evaluate trust level, confidence, and the derived relative trust—both for the whole service as well as parts of its security system (e.g., encryption). Bahtiyar and Çağlayan (2014) put particular emphasis on the fact that their system allows adjusting trust computations to the needs of the individual entities.

5.2 Reputation Models

5.2.1 *Accumulated Reputation Model.*

Yu et al. (2014a) (ID 13 in Table 6) present a novel reputation model showcasing that: unique environments sometimes cannot be treated with already existing models. Their focus is on participatory sensing systems, where high-quality sensing data are required, but which also suffers from a high degree of uncertainty (*mobile environment*) and malicious and inexperienced users. The authors reject several existing reputation models for similar environments like ad hoc (beta reputation) or wireless sensor networks (*Kohonen maps*).

Instead, Yu et al. (2014a) propose a new centralized, three-step approach. Pre-processing of the sensing data is conducted first. A density-based outlier detection is used to detect abnormal participants. Next, they compute a so-called contribution score with the sigmoid Gompertz function. It takes the value assigned by the outlier detection as an input and returns a value that will be used to weight the influence of a certain sensing result. Since the previous steps, especially the density-based algorithm, depend on a population of mostly normal participants, an additional reputation score is computed. Based on historical contributions and the trimmed mean method it computes an additional weighting factor.

Yu et al. (2014a) conducted a set of experiments with three different agent types, including normal ones, inexperienced, and malicious users. In the study, the ARM method was shown to be able to detect malicious sensing results with the contribution score—as long as their share is limited. For other cases, the reputation score has been shown to work, and comparison with other models is promising.

5.2.2 NDR and NDRU. The outstanding characteristic of the models proposed by Abdel-Hafez et al. (2015) (ID 14 in Table 6) is the fact that they aim at including the distribution of rating values when computing a reputation score. They claim that other factors like time would have been integrated already, while distribution has not, so that a rating set like $\{2, 2, 2, 2, 3, 5, 5\}$ might be averaged to “3” instead of “2,” which based on frequencies appears to be more suitable.

Based on their baseline models, the Leniency-Aware Quality Model (Lauw et al. 2012) and the multinomial Bayesian/Dirichlet probability distribution (Jøsang and Haller 2007), Abdel-Hafez et al. (2015) propose Normal Distribution Based Reputation Model (NDR). As weightings for their NDR method, the authors suggest the use of the normal distribution function, as they perceive ratings to be a normal, natural phenomenon. To do so, the ratings in the range of $[1, k]$ (*k being the number of rating levels*) are deployed over the index space $[0, n - 1]$. With the fixed mean $\mu = \frac{k+1}{2}$, the normal distribution density function can be set up to assign each rating a weighting. For each rating level (*e.g., one star, two stars, . . .*), the weightings are summed up and then used as a rating level weighting when computing the reputation from the ratings.

Since according to Abdel-Hafez et al. (2015) NDR is aimed at dealing with dense datasets, they propose NDR accounting for Uncertainty (NDRU) as an extension. NDRU brings together NDR and the Dirichlet method to account for uncertainty within the data. Doing so, NDRU is supposed to be slightly less optimistic, respectively, pessimistic than NDR. Subsequent evaluations measuring the accuracy of the computed reputation scores shows that NDRU provides the best overall performance, while NDR succeeds on dense and Dirichlet on sparse datasets.

5.2.3 Negative Multinomial Reputation. With their Negative Multinomial (NM) model, Wei and Wang (2014) (ID 15 in Table 6) address the implementation of a reputation system for self-organized networks. Since such networks are highly distributed and without fixed topologies, centralized control is difficult, and cryptography was unable to stop internal threats. Thus, they decided to implement a multinomial reputation model with additional discounting methods.

To classify behavior, Wei and Wang (2014) suggest the use of the Local Outlier Factor (LOF), which for a restricted entity neighborhood checks the degree of being an outlier. With a small example of a scenario with three influence factors, the authors were able to show the superiority of a multinomial over a binomial model.

Wei and Wang (2014) also point out the necessity to introduce a reputation discount factor. Due to the topology of a self-organized network, they see the risk that it might not be possible to capture the exact numbers for positive and negative outcomes. To account for this, they suggest recording the minimum number of each. As potential discount methods, Wei and Wang (2014) propose one based on the Mean Absolute Deviation (MAD) (*complex, for complete information*) and another one based on the NM parameters (*not complex, incomplete information*). The final evaluation reveals that the NM model delivers the desired results. It detects malicious entities faster than a normal binomial model and is better in fighting malicious entities success while supporting benign ones.

5.2.4 Vertical Handover Decision Making. The reputation model proposed by Giacomini and Agarwal (2013) (ID 20 in Table 6) can be understood as an extension paper to the one by Zekri et al. (2010) and aims at the improvement of the handover process in mobile networks. Instead of having a security focus as some of the other network/wireless oriented papers, Giacomini and Agarwal (2013) try to enhance the performance of the overall process.

In a first step, the authors explain the reputation system for Vertical Handover (VHO) proposed by Zekri et al. (2010), which they, later on, use as an input for their Grey System model. In this model, each mobile agent (*e.g., a smartphone*) has the ability to compute a score regarding the network state, considering the QoS in terms of bit error rate, delay, jitter, and bandwidth.

In a concluding evaluation, Giacomini and Agarwal (2013) test their improvements against the base model of Zekri et al. (2010). They conclude that their adjustments enhanced the output, since typically more scores for reputation are collected and the number of handovers has been reduced.

5.2.5 Anti-Distributed Voice Spam. Wang et al. (2013) (ID 21 in Table 6) proposed the Anti-Distributed Voice Spam (ADVS) model as a counter to Spam over Internet Telephony (SPIT), being delivered over distributed, self-organized VoIP networks without any central authority. They argued that a reputation-based model was necessary, since many of the existing strategies, such as list-based or content-based filtering, are non-functional. Nevertheless, Wang et al. (2013) identified two characteristics of SPIT that are rather simple to observe: the *call density* describing the number of calls in a short time frame and the *call length*, which is typically shorter for Spam calls.

The ADVS is conceptualized as a distributed reputation model, storing user reputation/evaluations in so-called Distributed Hash Tables (DHT). This way potential Denial of Service (DoS) attacks on centralized architectures should be avoided that otherwise would render the VoIP system defenseless.

Evaluation, carried out on a testbed developed by the authors themselves, was conducted to evaluate success rates. It revealed that the ADVS system was stable even with varying call densities and spammer shares, yet the detection rate developed best given high call densities (*many abilities to "learn"*).

5.2.6 ANN-based Reputation Bootstrapping. A reputation model specialized on solving the reputation bootstrapping issue is presented by Wu et al. (2015) (ID 22 in Table 6). In their application domain, Service-Oriented Computing (SOC), they observed that trust-related problems are a core issue that is not yet sufficiently fixed. Due to a lack of prior experience, such entities are often assigned default values leading to the dilemma that allocating a high value encourages identity changing and low reputation values handicap new services. Previously proposed bootstrap methods are rejected by Wu et al. (2015), as they claim that often the assumptions (*like endorsements*) behind ideas are unrealistic.

To fix the issue, Wu et al. (2015) propose what they call a generalization-based tentative reputation that bases on an ANN, as well as provider reputation as a surrogate for the performance of its new service.

In an evaluation against models assigning default reputation values (*minimum or average reputation*), the ANN-based reputation bootstrapping is superior. It also works given noise features (*features providing no insight*) as it just prolongs the time till the ANN converges.

5.2.7 Flow-Based Reputation with Uncertainty. Škorić et al. (2016) (ID 28 in Table 6) address the inability of flow-based reputation models such as EigenTrust or PageRank to account for uncertainty as well as the structural dependency of trust networks by "merging" both approaches together. For this purpose, Škorić et al. (2016) propose a new Evidence-Based Subjective Logic (EBSL) operator. Subsequently, the authors show the viability of their combined flow-based reputation and subjective logic model with some experiments. They point out that the system can account for uncertainty while accommodating arbitrary trust networks.

5.2.8 Eigentrust Dynamic Evolutionary Model in P2P. In their publication, Lu et al. (2016) (ID 32 in Table 6) challenge the traditional assumption of (P2P) reputation systems that peers are altruistically providing their services. Hence, the authors developed their reputation model in a fashion that, e.g., allows to punish peers not offering own content as defective peers. Furthermore, Lu et al. (2016) use game and evolutionary theories to model the adaptive behavior of peer agents so that they can adapt to promising strategies. The derived insights are subsequently implemented on top of the existing EigenTrust reputation management system.

5.2.9 A Topic-Biased User Reputation Model in Rating Systems. Following their observation that user reputations—and the linked item scores—in e-commerce product review systems are highly topic dependent, Li et al. (2015) (ID 35 in Table 6) propose to improve the ratings by incorporating the topic as an additional variable. For this purpose, the authors generalize six existing reputation algorithms into so-called topic-biased algorithms, as visualized in Equation (1)[6]:

$$L_1^{\max} = \lambda \max_{o_j \in N_i} |R_{ij} - r_j^{s+1}| \quad \rightarrow \quad TB - L_1^{\max} = \lambda \max_{o_j \in N_i} b_{jk} |R_{ij} - r_j^{s+1}|. \tag{1}$$

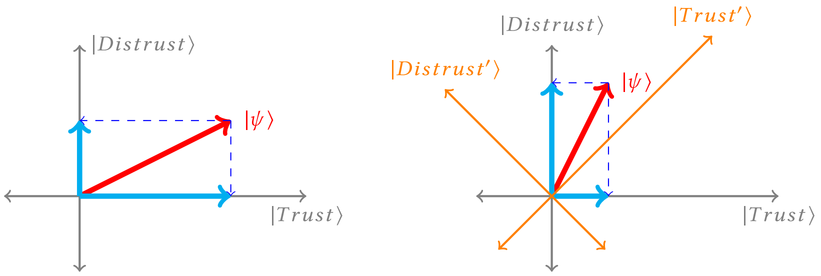
There the topic-bias is introduced by adding b_{jk} as the degree to which object o_j belongs to a topic t_k. The authors point out that topic-bias can similarly be introduced into a large set of different user reputation algorithms.

5.2.10 Utility-Based Reputation Model for Grid Resource Management. Differing from many of the other presented approaches, Kussul et al. (2015) (ID 39 in Table 6) do not present an entirely new system but extend an already existing system (Arenas et al. 2008, 2010). Focussing on the domain of grid computing and virtual organizations enhance an existing reputation model by incorporating time decay of reputation, the ability to consider collusion and to assign initial reputation values to new grid resources (as to resolve the cold start problem). In addition, Kussul et al. (2015) adapt the user reputation model SMUB (Kussul and Skakun 2004, 2005; Skakun and Kussul 2006; Skakun et al. 2005) to the grid computing domain to better account for user behavior. Both values are then used in combined fashion to improve grid job scheduling in a way that allows disregarding both untrustworthy resources and users.

5.3 Hybrid Models

5.3.1 Quantum-Like Formulation of Computational Trust. A rather special model is proposed by Ashtiani and Azgomi (2014) (ID 1 in Table 6) who aim at tackling the issue of computational trust by quantum theory. To ground and justify their research, they provided six gaps left by current models. These include the so far separated handling of trust and distrust, ignorance of side-effects (*bias, irrationality, order effect*) and the misrepresentation of context. Furthermore, the role of subjective bias and the lack of research concerning exploration vs. exploitation are criticized.

[6] R_{ij} represents the rating of item o_j by user u_i; r_j^{s+1} refers to the item score of object o_j in step $s+1$; λ is a damping factor.



(a) Trust Vector in Context Space.

(b) Context Change.

Fig. 5. Context as vectors (Ashtiani and Azgomi 2014).

Ashtiani and Azgomi (2014) tackle the first gap by expressing a state (vector) via quantum probability theory $|\psi\rangle = \alpha_0 |distrust\rangle + \alpha_1 |trust\rangle$,[7] which shows that both components are always simultaneously considered. The model represents context via quantum contextuality, which comes down to the set of basis vectors. Context changes are then conceptualized via transformations and rotation of these vectors (see Figures 5(a) and 5(b)).

Ashtiani and Azgomi (2014) conducted several experiments to showcase that their new model—especially the bias-related components—were able to improve prediction quality. This includes demonstrations regarding the filtering of malicious entities, as well as scenarios dealing with exploration vs. exploitation. The authors also use the experiments to point out the adjustability of their new model.

5.3.2 Wierzbicki et al. The approach by Wierzbicki et al. (2013) (ID 3 in Table 6) is quite different from *StereoTrust*. Their first step is explaining a perceived weakness they claim to have found in other trust and reputation models. According to their paper, most of the approaches use only simple numeric/Likert scales, which they deem insufficient to handle the complex multi-criteria nature of trust/reputation. Furthermore, they assume that people—especially for negative ratings—tend to add additional textual information if possible.

Wierzbicki et al. (2013) propose a new trust model and trust management system. They suggest analyzing Internet auction traces to obtain user behavior information. These information are then used to generate so-called proofs $p^{AB} = \{c, \{l_i, s_i\}^m_{(i=1)}\}$, which analyze the user behavior l_i (with strength s_i) between a trustor agent A and a trustee agent B in a given context c. Based on the proofs they define an aggregation and a selection operator. The first uses the empirical distribution to average the valuations s_i of each label l_i. Doing so they compute the strength of the aggregated proof p^{AB}_{agg}, for example to summarize all proofs of one or different trustors to a single trustee B. For the computation of the aggregated strength s_i^{agg} special attention is paid to increase the impact of extreme values. The selection operator enables the creation of a proof ranking allowing the selection of the most relevant one. To achieve this it scales the strength values s_i to be able to select (weakly) Pareto optimal solutions. Selecting a Pareto optimal solution provides the benefit of having a solution that is "*ideal*" according to multiple targets/contexts.

5.3.3 3-R. The 3-R model has been proposed by Majd and Balakrishnan (2015) (ID 7 in Table 6) aiming at the evaluation and selection of trustworthy agents in MAS environments, which they perceive as next-gen computing. 3-R stands for the three major components of their model:

[7] Trust itself is defined as the quintuple $Trust(X, Y, C, \tau, g)$ with X being the trustor, Y the trustee, C the context, τ the actions, and g the goal of the trustor. ψ in this case is the assigned name of the computed states, while α_0 and α_1 are complex numbers (Nielsen and Chuang 2011).

reliability, *reputation*, and *risk of interactions*. Majd and Balakrishnan (2015) suggest using them to deal with the particular situation of a buyer lacking prior experiences with a potential seller.

Simulations using different distributions and groupings of beneficial and malevolent agents yielded the desired result: Benevolent agents received higher scores for reliability, reputation, and belief, while risk and disbelief were higher for malicious agents.

5.3.4 DISARM. The DISARM method proposed by Kravari and Bassiliades (2016) (ID 9 in Table 6) is a distributed reputation model that is explicitly aimed at MAS. They suggest the use of a distributed system using personal as well as witness information together with Defeasible Logic (DL). Interestingly, the DISARM approach is one of the few approaches that is provided with a computational complexity analysis.

Apart from the central element of distribution, DISARM has five additional principles. This includes the usage of time and rating quality as influence factors, as well as using black- and whitelists to handle special partners. The importance of interactions, as well the confidence with them, are the remaining suggestions. Based on these principles, a set of rating parameters is derived, including items like response time, validity, correctness, confidence, and a time stamp.

The conducted evaluations revealed that DISARM is delivering good utility and also able to compete with different solutions regarding the reputation issue.

5.3.5 Comprehensive Reputation. Yan et al. (2015) (ID 10 in Table 6), the authors of the Comprehensive Reputation (CR) model, start their paper with an extensive overview of potential threats in an e-commerce setting as well as with existing reputation models. To address these, they suggest the use of social information like the social context or existing relationships between agents. Yet, even here, Yan et al. (2015) find critical issues like the identity shift problem (which refers to the fact that agents can easily change their ID/username and thus reappear with a new, yet unsullied identity), imbalance vote bias, winner circle bias, and the early bird bias.

To account for the discovered problems, Yan et al. (2015) deem it fit to propose a new, graph-based model for comprehensive reputation, making use of multiple trust sources and inter-user links including their values and context. The previously identified issues are reduced to three challenges the new model should address: the *veracity of opinions* (malicious agents misleading user), the *subjectivity of opinions* and *dynamics of behavior*.

Yan et al. (2015) suggest the computation of two major reputation scores: behavior reputation and social relationship reputation.

Both social relationship reputation and behavior reputation are aggregated to the CR score of the evaluated agent.

To improve their model, Yan et al. (2015) propose three additional enhancements. The first is a Theory of Reasoned Action (TRA) and Expectation-Confirmation Model (ECM) based filter for bad-mouthing ratings. Second and associated third suggestion is a maximum risk tolerance, respectively, a personalized MRT to have a clear indicator of which amount of risk will be taken. The conducted evaluation provides evidence that the concept works but also reveals that it performs best in environments with many defecting agents.

5.3.6 Ransi and Kobti. Differing from many of the other presented approaches, Ransi and Kobti (2014) (ID 11 in Table 6) provide both a reputation as well as a trust model. Regarding their reputation model, they point out that it was unique regarding using direct interaction and witnesses as information sources. The underlying rationale according to Ransi and Kobti (2014) is that direct interaction provides reliable information, whereas witness information is less scarce. Under these circumstances, the authors point out the necessity to weight direct information higher, since its usual quality was supposed to be superior. From the architectural perspective, they decided to use a centralized architecture that collects the ratings after each transaction to compute centrally available reputation scores. Each rating in Ransi and Kobti (2014) model is, in fact, a triplet, evaluating *item described*, *performance* and *arrival time* with the values 0 (*bad*), 1 and 2 (*best*). The agent landscape is rather simple, with only two agent types being used (providers and consumers) and the cold start problem being solved by letting consumers interact with all providers to collect experience.

An evaluation comparing the hybrid approach to a direct information and witness information is the only approach reveals the superiority of the hybrid over both methods. To conclude their paper, Ransi and Kobti (2014) propose an additional trust model, which is aimed at private, non-business users. It simply computes the trust value as the sum of all ratings of a provider divided by the interactions conducted.

5.3.7 *Kussul et al.*

For their reputation model, Kussul et al. (2013) (ID 12 in Table 6) have selected a rather rare focus, by evaluating resistance to common threats and attacks on such models instead of their performance. The application domain for which they develop this model is the area of grid computing, which is characterized by distributed and heterogeneous resources.

First, Kussul et al. (2013) adjust a provider reputation model, which they claim to have taken from Arenas et al. (2008, 2010). The utility-based model originally uses Service Level Agreements (SLA) to measure utility and feeds the respective functions with events that are a tuple of different variables (*e.g., time, user, resource, etc.*). In case a SLA is violated, a penalty value is added. As a threat/attack countermeasure, they add three functions that should prevent consumer-resource alliances, ensure time-decay valuation and the assignment of different ratings to different services. Based on the utility values, reputation is computed as the expected value of the utility function.

As a second reputation model, a user reputation model is introduced that should check for and punish users violating Virtual Organization (VO) policies. Here they base their work on the Statistical Model of User Behavior (SMUB) research they claim to have conducted earlier. It accounts for a larger set of parameters like job site, execution target, CPU time, and job exit status.

For the conducted evaluation the reputation score was integrated into the grid scheduler to have a multi-criterion scheduling system. Subsequent tests showed that the reputation system was able to detect malicious nodes and to detect and fight several of the presented threats.

5.3.8 *Chang et al.*

A model that is explicitly aimed at supply chains, respectively, the phase of Supply Chain (SC) formation (*determining partners*) is presented by Chang et al. (2014) (ID 16 in Table 6). They claim that SCs are increasingly turning into VOs on the Internet, partly due to the need for speed only achievable by digitization, yet without trust in such relationships being sufficiently researched so far.

Since Chang et al. (2014) perceived binomial trust and reputation (*good vs. bad*) as insufficient, they proposed seven new trust indicators to establish a multi-dimensional approach. Five of these indicators capture subjective feelings of a customer (*rater*), like price and quality feedback regarding products and services and the delivery time. Two additional ones capture supplier characteristics, like the size and market share.

Based on these indicators, Chang et al. (2014) propose the reputation based decision model. The first step regards collecting feedback in the form previously defined indicators. Here, Chang et al. (2014) include both individual reputation based on direct information as a reliable input and witness reputation based on indirect information to provide a broader data basis. For both reputation parts, a time-decay function is applied before the single items are aggregated via the weighted average. If both are available, then the final reputation includes both; otherwise, only the available reputation parts are integrated.

For the final decision, Chang et al. (2014) propose a multi-criteria decision-making model to add the ability to consider even more criteria than just reputation. First, a set of axioms is presented that the model components have to fulfill (*e.g., weights being continuous and monotonically increasing*). If a certain amount of properties fulfill the threshold, then the underlying set is called a satisfaction choice. From this set, the model then computes a state and a weight vector, which is used to make a final decision. With the so-called "*one-vote vetos,*" Chang et al. (2014) add a special functionality that automatically prevents the interaction with a supplier, if a certain variable has not reached a certain threshold (*e.g., price too high*). The final evaluation of the model indicated that the k-means filter can separate unfair ratings and that the one-vote veto has a strong impact, as it makes reputation and trust much less influential.

5.3.9 Dynamic Selection of Reputation Mechanism. In contrast to most of the other analyzed approaches, Tormo et al. (2015) (ID 17 in Table 6) do not present a new trust or reputation model but rather a tool that allows one to dynamically select a suitable algorithm from a pool of existing ones. They justify this concept by pointing out that environments like Internet of Things (IoT) are extremely dynamic, whereas most available reputation/trust models hardly offer any options to adjust them to different situations.

The engine selection is built on fuzzy sets and inference rules (*with a set of linguistic labels for interpretability*), since Tormo et al. (2015) found them to be more flexible than classical sets (*rules can easily be extended by adding additional conditions etc.*). Input data includes the current system conditions as well as performance measurements representing the desired state.

Since running all engines in parallel would be too computationally complex, Tormo et al. (2015) additionally provide a smooth transition functionality as a newly started reputation engine might have to be initialized first. Thus, for a limited amount of time, two engines run in parallel providing dynamically weighted contributions to the overall reputation, before finally only the currently selected engine runs alone.

5.3.10 RPRep. Similar to the research by Kussul et al. (2013), Wang et al. (2016) (ID 18 in Table 6) also present a model that is tailored to counter what they call tactical attacks and a Vehicular Ad Hoc Network (VANET) specific attack, the so-called reputation link attack. They point out that VANETs so far have been secured via firewalls and access control against external attackers, yet internal attackers have not been considered sufficiently.

RPRep distinguishes two distinct message reputation types, one for services and another one for feedback. To mitigate the above-mentioned attacks, each feedback rating has to fulfill requirements. Feedback on service reputation is checked via information entropy to discover collusion attacks.

To counter the reputation link attacks, Wang et al. (2016) present the hidden zone and k-anonymity approach. In the first method, protection is achieved by hiding reputation values in a mix-zone (i.e., are areas where multiple vehicles concentrate (*e.g., traffic lights*). That way tracking for an attacker (*who is only able to observe local values*) is only possible if it follows a target out of the zone. To prevent attacks by attackers monitoring large areas (*global attackers*), k-anonymity assigns k-vehicles the same reputation value/range. The evaluation conducted by Wang et al. (2016) shows that the tactical attacks can be fought successfully and that k-anonymity is sufficient to block global attackers, while against local attackers a combo together with the hidden zone delivered the best results.

5.3.11 DSCS and DCSA. With the Distributed Secure Cooperative Sensing (DSCS) and the Distributed Cheat-Proof Spectrum Allocation (DCSA) strategies, Lin et al. (2015) (ID 19 in Table 6), similar to Kussul et al. (2013) and Wang et al. (2016), propose another strategy explicitly focused on attacks and threats in a rather special environment, namely Cognitive Radio Networks (CRN). The main concern in this domain is organizing the frequency sharing between different users. so-called secondary users can exchange sensing results to improve their frequency detection performance. However, this makes them vulnerable to internal attacks.

As a first step, the DSCS approach is suggested by Lin et al. (2015) to prevent attacks on the actual sensing phase. The strategy makes use of subjective logic (Jøsang and Hayward 2006), which captures an opinion via a four-tuple $\omega_{x:y} = \{b_{x:y}, d_{x:y}, u_{x:y}, a_{x:y}\}$ containing an entity x's belief, disbelief, uncertainty and base willingness to believe toward an entity y. As each entity will typically have multiple opinions from recent interaction, these will be aggregated into a single opinion. Moreover, the opinions from prior points of time can be added to the final reputation, yet only after applying a time decay function on the values. Once the probability expectation value of a tuple of the final reputations falls below a threshold, the three entities with highest trustworthiness/reputation are selected to search frequencies.

To prevent attacks on frequency allocations, Lin et al. (2015) add the DCSA strategy, based on the Vickrey-Clarke-Groves (VCG) mechanism, as a check-proof allocation strategy. DCSA first measures a user's and a system's profit by weighting throughput based utility against reputation based cost. In a next step, taxes are introduced depending on requested capacity per agent. This way DCSA fulfills the VCG requirement of incentive compatibility and individual rationality, as requesting more capacity than needed becomes unattractive. The concluding evaluation revealed that especially DSCS has benefits in finding signals and mitigating attacks, whereas DCSA to a certain degree depends on the careful work of the DSCS.

5.3.12 Fuzzy-Logic Based Trust and Reputation Model. Chandran et al. (2016) (ID 23 in Table 6) propose a novel trust and reputation model to improve the security of resource allocation in cloud environments. Similar to Hammer et al. (2015), Chandran et al. (2016) do not consider an agent-agent interaction, but how a system can use user-feedback to assess the trustworthiness and reputation of a cloud resource. The collected trust and reputation values of the resource are fed into a fuzzy logic model as well as a shallow neural network. Subsequently, the values are merged via a weighted average. Chandran et al. (2016) then use the score and a threshold to determine suitable, secure cloud services. Their evaluation is conducted on three distinct data sets and up to 250 users—however, only a little information is provided on dataset structure and experimental setup.

5.3.13 Hesitant Fuzzy Model of Computational Trust. In their second computational trust model, Ashtiani and Azgomi (2016b) (ID 24 in Table 6) address five distinct open issues: Those comprise the typical quantitative representation of trust, the inability to capture context, vagueness, and uncertainty, as well as the failure of most models to account for recommender taste and changes of personality. Since Ashtiani and Azgomi (2016b) observed (human) agents suffering from quantifying their satisfaction, they propose to use fuzzy linguistic terms (see Equation (2)), which they convert to "hestitant fuzzy linguistic term sets" (see Equation (3)). Furthermore, Ashtiani and Azgomi (2016b) allow trust to be composed of multiple—user-definable—criteria. Given their usage of recommender agents to evaluate potential trustee agents, Ashtiani and Azgomi (2016b) add vagueness and certainty evaluations to assess the quality of recommendations. On top similarity with trustor assessments and changes over time are considered to devaluate malicious or different thinking recommenders. A suitable trustee is selected based on non-dominance choice degree representing one of the final steps in the 13-step approach of Ashtiani and Azgomi (2016b):

$$p_f^i = \begin{bmatrix} - & \text{lower than high} & \text{low} \\ \text{greater than medium} & - & \text{at most medium} \\ \text{at least high} & \text{between very low and medium} & - \end{bmatrix}, \tag{2}$$

$$p_f^i = \begin{bmatrix} - & \{\text{neither, very low, low, medium}\} & \\ \{\text{high, very high, absolute}\} & - & \{\text{neither, very low, low, medium}\} \\ \{\text{high, very high, absolute}\} & \{\text{very low, low, medium}\} & - \end{bmatrix}. \quad (3)$$

5.3.14 Type-2 Fuzzy Logic-Based Framework for Reputation Management. In their 2016 Information Science publication, Acampora et al. (2016) (ID 25 in Table 6) propose another fuzzy logic reputation model tailored for the domain of peer-to-peer (P2P) e-commerce. After each trade transaction, a trust value is computed for each agent evaluating its performance as a seller or buyer and then also sent to the respective peer agent. Furthermore, each agent computes its reputation based on feedback from other peers it interacted with previously—considering the credibility regarding the proximity of their opinion to the actual reputation values in prior transactions. To improve the handling of uncertainty and vagueness prevalent in P2P systems, Acampora et al. (2016) use Interval Type-2 Fuzzy Sets to add additional degrees of freedom. They use a precision- and recall-based evaluation with eBay and simulated data to indicate their systems superiority over conventional ones such as EigenTrust, PeerTrust or eBay.

5.3.15 Filtering Trust Opinions Through Reinforcement Learning. With the Actor-Critic Trust (ACT) model, Yu et al. (2014c) (ID 26 in Table 6) provide a novel computational trust model to deal with malicious agents as well as the necessity of previous trust models to manually tune parameters to detect such agents. For this, the actor-critic reinforcement learning method is used. By comparing received recommendations of other agents with the actual outcome of the transaction allows the method to learn an appropriate weighting for the recommending peers. Beyond strict exploitation, the ACT model also enables exploration of new assessors for which no prior information is available.

5.3.16 Reputation-Based Bootstrapping Mechanism. Working in the domain of intrusion detection systems (IDS) and collaborative alert systems (CAS), Pérez et al. (2014) (ID 27 in Table 6) introduce a novel reputation model that is specifically tailored to the assignment of initial reputation scores to newcomers. The offered reputation score heavily depends on detection skills a newcomer (device) can and is willing to offer to the IDS, respectively, CAS. Depending on the type of device (mobile or static or new security domain) and entrance to the network (complete newcomer or re-entrance) the applied algorithms slightly differ.

5.3.17 FIRE+—Multidimensional Decentralized Trust and Reputation Model. Based upon the existing FIRE trust and reputation model (Huynh et al. 2006), Qureshi et al. (2013) (ID 29 in Table 6) propose a novel model version to deal with malicious and collusive agents. Using both direct and indirect trust information for the computational model, Qureshi et al. (2013) use this information to uncover the likelihood of agent collusion. An indicator for such behavior may be the comparatively high number of recommendations from a subset of agents toward a specific trustee that goes far beyond the number of recommendations from other agents toward that trustee. Furthermore, Qureshi et al. (2013) use transaction history information to determine the confidence to be placed into trust and reputation scores based on the number and quality of prior transaction experiences.

5.3.18 Combination Trust Model for Multi-Agent Systems. A computational trust model for multi-agent systems is proposed by Nguyen and Tran (2013) (ID 30 in Table 6). Similar to many of the other—and typically later—publications, Nguyen and Tran (2013) make use of trust information from both direct experiences as well as second-hand information. While the authors consider a time decay factor as well as different weighting strategies between direct and indirect trust values, the proposed model lacks a handle for malicious agents by assuming their trustworthiness. Based on their model evaluations, Nguyen and Tran (2013) suggest always to consider both trust sources for decision making. For the sharing of reputation information, they deem sharing the full and direct-only trust information as viable.

5.3.19 Computational Dynamic Trust Model for User Authorization. Zhong et al. (2015) (ID 36 in Table 6) propose a computational dynamic trust model intended for usage in resource selection for P2P systems or ad hoc networks. In this model, Zhong et al. (2015) distinguish integrity and competence trust: The former refers to the general, non-context-dependent belief in the honesty of a trustee with a large amplitude over time, whereas the latter relates to the context-dependent belief in a trustee's abilities and expertise, which has been found to be slightly steady. Via the inclusion of predictability—assessing the variability of trustee behavior and the number of prior transactions—a confidence value is added for each trust score. Wherever direct assessments are not available, Zhong et al. (2015) fall back to using reputation values collected from other agents. For the different setups, e.g., the presence or absence of direct information or a focus on shared beliefs, Zhong et al. (2015) provide different methods to compute the trusting beliefs.

5.3.20 Trust and Reputation Model for Robotic Sensor Networks. To encounter the risks and uncertainties associated with the deployment of robotic sensor networks (RSNs), Tuna et al. (2013) (ID 40 in Table 6) propose a corresponding trust and reputation model. Their five-stepped model mostly uses reputation information collected from nodes in a given RSN to select a suitable service providing node. Here, evaluation quality is improved by Tuna et al. (2013) via the inclusion of confidence levels, respectively, credibility of the informing nodes. All potential service providing nodes are globally ranked based on their aggregated reputation value, and the consuming service agent subsequently evaluates the selected node. Given the need to minimize energy consumption and bandwidth in RSNs enhance their model by incorporating additional steps to aggregate exchanged information.

6 CONCLUSIONS

While this article is long, it feels short given the complexity of the underlying topic as well as the extensive amount of research already conducted; here, we subsume some conclusions that can be drawn from it.

The first contribution of this article is the provision of extensive definitions for the concepts of *Trust* and *Reputation*. Since researchers over the past 25 years were unable to agree on a standard definition, it appears to be necessary as well as valuable to present a detailed analysis on the state of research. By doing so the reader is expected to gain a good understanding on the relevant concepts, including potential gaps helping him to get a better grip on potential inconsistencies in the existing computational trust and reputation models. Furthermore, the review gives additional definitions for computational trust and computational reputation, to provide a clear differentiation as well as a cognitive link between the original human concept and its digital adaptation. As a complement, an overview of the relationship between trust and reputation is provided to enable the reader better understanding of the ambiguous link between the two ideas.

The second contribution—and most important—is the creation of a new schematic/matrix review scheme to assess (computational) trust and reputation models. For this aim, some of the most influential and most cited review papers in this academic area (Pinyol and Sabater-Mir 2013b; Sabater and Sierra 2005) have been analyzed. To integrate the existing approaches, their most distinctive characteristics were extracted and merged into a new review scheme. Some additional concepts reoccurring in related literature but so far not present in review studies have been added to put the maximum amount of insight into the created matrix scheme. The rationale for the provision of such an extensive tabularized matrix lies in the idea of enabling the quickest possible assessment of a maximum amount of research.

As a final—and second major contribution—40 recent computational trust and reputation models have been evaluated. This enabled us to help bridging the gap between the last past review papers by Pinyol and Sabater-Mir (2013b) and Yu et al. (2013) to the current day. Considering the high amount of activity exhibited on these research topics, which demands a regular update on the latest models to appear for one to keep track of the ongoing developments. Furthermore, we think this work, especially the put forward review matrices, enables a quick yet effective access to a large set of highly relevant research.

Beside these conceptual contributions, the present survey allowed some insightful delving into the current state of research. The analysis revealed that certain characteristics, such as the use of multiple input sources, consideration of cheating, hybrid approaches (*trust and reputation*) as well as the provision of procedural and cognitive concepts have apparently become common, which is good in a research area that has not a good record of consensus. MAS, often mentioned in close relationship with computational trust and reputation, are shown to be a well-used concept. However, the review indicates that other approaches like ANN or SVM should also be taken into consideration.

While some aspects of research regarding trust and reputation apparently start to converge, important issues such as how to aggregate trust and reputation or how to select a suitable partner are still vividly discussed. In these aspects, the 40 reviewed papers show the least commonalities. Moreover, some elements like computational efficiency and standardized testbeds (*or real-world data*) are not yet considered, which is interesting considering the IoT or mobile devices. Also, issues regarding comparability should be taken on board. The lack of any kind of reference model so far is a striking observation given the fact that researchers have been tackling these topics for more than 25 years.

For the sake of completeness, it has to be mentioned that this survey has some limitations. One of them is that even despite deemed as a useful tool for research, the matrix scheme was difficult to apply on all analyzed research papers. Typically, non-standardized vocabulary is used, which makes it cumbersome to assign an appropriate value to each analyzable characteristic. Part of the problem might be the fact that the reviewed models deal with multiple aspects of the computational trust and reputation domain, such as, model bootstrapping, security concerns and domain specific issues. Multiple different matrix schemes would have been the perfect fit, which, however, was undesirable as it would lose the advantage of comparability.

This systematic literature review has been focused on considering only journal publications, since these usually undergo the most extensive review and revision cycles. Hence, journal articles typically represent the primary venue for searching (high) quality research. Also, their usual rather extensive length makes a review and summarization valuable. For the future, we intend to extend our review to include the more fast-paced conference proceedings—especially those exhibiting high impact in the domain of trust and reputation research (e.g., International Conference on Autonomous Agents and Multiagent Systems (AAMAS); Association for the Advancement of Artificial Intelligence (AAAI); International Joint Conference on Artificial Intelligence (IJCAI); IEEE International Conference on Web Services (ICWS), IEEE International Conference on Services Computing (SCC); International Conference on Service-Oriented Computing (ICSOC); The International World Wide Web Conference (WWW), etc.).

From these observations and limitations, a new set of future research directions can be derived. This, namely, the creation of the first reference model, appears to be beneficial. This might help to avoid creating new models without reconciling with already conducted research. An additional interesting move would be the creation of standardized (*real-world data*) testbeds. Those would be extremely beneficial regarding comparability. Even though (computational) trust and reputation are both expressed in extensive definitions like the ones presented in this article, another potential direction for future research would be to rethink the way of defining those concepts. While up to now considered as large, monolithic concepts, rethinking them with regard to the application domains and its problems may prove to be inherently valuable. It would allow more concise and actionable specifications tailored to the specifics of each field. With this contribution focusing on the conceptual level of (computational) trust and reputation models created and used in recent research, it would be desirable for future publications to provide additional analysis of the actual implementations and the underlying technical perspective. Ideas for such a contribution include, but are not limited to, the provision of complexity analyses, an overview overused network topologies for trust/reputation information exchange as well as implemented APIs to existing systems. The last and maybe the most utopic idea drawn from this long reader would be the design of a standardized vocabulary based on the already proposed review schemes, to enable a discussion liberated from terminological misunderstandings.

ELECTRONIC APPENDIX

The electronic appendix for this article can be accessed in the ACM Digital Library.

ACKNOWLEDGMENTS

We thank the editor and anonymous referees of this journal whose comments substantially improved this article.

REFERENCES

Ahmad Abdel-Hafez, Xiaoyu Tang, Nan Tian, and Yue Xu. 2014. A reputation-enhanced recommender system. In *Advanced Data Mining and Applications*, Xudong Luo, Jeffrey Xu Yu, and Zhi Li (Eds.). Springer, Cham, 185–198. DOI: https://doi.org/10.1007/978-3-319-14717-8_15

Ahmad Abdel-Hafez, Yue Xu, and Audun Jøsang. 2015. A normal-distribution based rating aggregation method for generating product reputations. *Web Intell.* 13, 1 (Apr. 2015), 43–51. DOI: https://doi.org/10.3233/WEB-150306

Alfarez Abdul-Rahman and Stephen Hailes. 2000. Supporting trust in virtual communities. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Vol. 1. IEEE Computer Society, 9. DOI: https://doi.org/10.1109/HICSS.2000.926814

Giovanni Acampora, Daniyal Alghazzawi, Hani Hagras, and Autilia Vitiello. 2016. An interval type-2 fuzzy logic based framework for reputation management in Peer-to-Peer e-commerce. *Info. Sci.* 333 (2016), 88–107.

Anna A. Adamopoulou and Andreas L. Symeonidis. 2014. A simulation testbed for analyzing trust and reputation mechanisms in unreliable online markets. *Electron. Commerce Res. Appl.* 13, 5 (Sep. 2014), 368–386. DOI: https://doi.org/10.1016/j.elerap.2014.07.001

Muhammad Aurangzeb Ahmad. 2012. *Computational Trust in Multiplayer Online Games.* PhD Thesis. University of Minnesota. DOI: http://purl.umn.edu/127398

George A. Akerlof. 1970. The market for "Lemons": Quality uncertainty and the market mechanism. *Quart. J. Econ.* 84, 3 (1970), 488–500. DOI: http://www.jstor.org/stable/1879431

Alvaro Arenas, Benjamin Aziz, and Gheorghe Cosmin Silaghi. 2008. Reputation management in grid-based virtual organisations. In *Proceedings of the International Conference on Security and Cryptography.* 538–545. Retrieved from http://eprints.port.ac.uk/5551/1/Reputation_Management_in_Grid-based_Virtual_Organisations.pdf.

Alvaro E. Arenas, Benjamin Aziz, and Gheorghe Cosmin Silaghi. 2010. Reputation management in collaborative computing systems. *Secur. Commun. Netw.* 3, 6 (Nov. 2010), 546–564. DOI: https://doi.org/10.1002/sec.146

Mehrdad Ashtiani and Mohammad Abdollahi Azgomi. 2014. Contextuality, incompatibility and biased inference in a quantum-like formulation of computational trust. *Adv. Complex Syst.* 17, 5 (Oct. 2014), 1–61. DOI: https://doi.org/10.1142/S0219525914500209

Mehrdad Ashtiani and Mohammad Abdollahi Azgomi. 2016a. A formulation of computational trust based on quantum decision theory. *Info. Syst. Front.* 18, 4 (2016), 735–764.

Mehrdad Ashtiani and Mohammad Abdollahi Azgomi. 2016b. A hesitant fuzzy model of computational trust considering hesitancy, vagueness and uncertainty. *Appl. Soft Comput.* 42 (2016), 18–37.

Şerif Bahtiyar and Mehmet Ufuk Çağlayan. 2014. Trust assessment of security for e-health systems. *Electron. Commerce Res. Appl.* 13, 3 (2014), 164–177.

Tina Balke, Stefan König, and Torsten Eymann. 2009. A Survey on Reputation Systems for Artificial Societies. Retrieved from https://www.econstor.eu/dspace/bitstream/10419/52616/1/612285189.pdf.

Jörg Becker, Daniel Beverungen, and Ralf Knackstedt. 2008. Reference models and modeling languages for product-service systems status-quo and perspectives for further research. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS'08)*. IEEE, 105–105. DOI:https://doi.org/10.1109/HICSS.2008.369

Amir Jalaly Bidgoly and Behrouz Tork Ladani. 2015. Modelling and quantitative verification of reputation systems against malicious attackers. *Comput. J.* 58, 10 (Oct. 2015), 2567–2582. DOI:https://doi.org/10.1093/comjnl/bxu130

Amir Jalaly Bidgoly and Behrouz Tork Ladani. 2016. Benchmarking reputation systems: A quantitative verification approach. *Comput. Hum. Behav.* 57 (Apr. 2016), 274–291. DOI:https://doi.org/10.1016/j.chb.2015.12.024

Rachel Botsman. 2015. The changing rules of trust in the digital age. *Harvard Bus. Rev.* (2015). Retrieved from https://hbr.org/2015/10/the-changing-rules-of-trust-in-the-digital-age.

Rachel Botsman. 2016. New trust networks: Your best friend is a stranger. *WIRED* (2016), 89–90. DOI:http://rachelbotsman.com/wp/wp-content/uploads/2016/01/Rachel-Botsman-in-WW2016.pdf.

John S. Breese, David Heckerman, and Carl Kadie. 1998. Empirical analysis of predictive algorithms for collaborative filtering. In *Proceedings of the 14th Conference on Uncertainty in Artificial Intelligence*. Morgan Kaufmann Publishers Inc. 43–52. DOI:http://dl.acm.org/citation.cfm?id=2074094.2074100

Andreas Brinkhoff, Özalp Özer, and Gökçe Sargut. 2015. All you need is trust? An examination of inter-organizational supply chain projects. *Prod. Oper. Manage.* 24, 2 (Feb. 2015), 181–200. DOI:https://doi.org/10.1111/poms.12234

Christopher Burnett. 2011. *Trust Assessment and Decision-Making in Dynamic Multi-Agent Systems.* PhD Thesis. University of Aberdeen. Retrieved from http://www.bcs.org/upload/pdf/dd-christopher-burnett.pdf.

Cristiano Castelfranchi and Rino Falcone. 1998. Principles of trust for MAS: Cognitive anatomy, social importance, and quantification. In *Proceedings of the 3rd International Conference on Multi Agent Systems.* IEEE Computer Society, 72–79. DOI:https://doi.org/10.1109/ICMAS.1998.699034

Federico Cerutti, Lance M. Kaplan, Timothy J. Norman, Nir Oren, and Alice Toniolo. 2015. Subjective logic operators in trust assessment: An empirical study. *Info. Syst. Front.* 17, 4 (Aug. 2015), 743–762. DOI:https://doi.org/10.1007/s10796-014-9522-5

Kamalanathan Chandran, Valarmathy Shanmugasudaram, and Kirubakaran Subramani. 2016. Designing a fuzzy-logic based trust and reputation model for secure resource allocation in cloud computing. *Int. Arab J. Inf. Technol.* 13, 1 (2016), 30–37.

Liu Chang, Yacine Ouzrout, Antoine Nongaillard, Abdelaziz Bouras, and Zhou Jiliu. 2014. Multi-criteria decision making based on trust and reputation in supply chain. *Int. J. Prod. Econ.* 147 (Jan. 2014), 362–372. DOI:https://doi.org/10.1016/j.ijpe.2013.04.014

Theodore H. Clark and Ho Geun Lee. 1999. Electronic intermediaries: Trust building and market differentiation. In *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences—Volume 5.* IEEE Computer Society, 1–10. DOI:https://doi.org/10.1109/HICSS.1999.772939

Harris Cooper, Larry V. Hedges, and Jeffrey C. Valentine. 2009. *The Handbook of Research Synthesis and Meta-Analysis.* Russell Sage Foundation. Retrieved from http://www.jstor.org/stable/10.7758/9781610441384.

António Aguiar Costa and Luís Valadares Tavares. 2013. Advanced multicriteria models to promote quality and reputation in public construction e-marketplaces. *Auto. Construct.* 30 (Mar. 2013), 205–215. DOI:https://doi.org/10.1016/j.autcon.2012.11.029

Pasquale De Meo, Fabrizio Messina, Domenico Rosaci, and Giuseppe M. L. Sarné. 2014. Recommending users in social networks by integrating local and global reputation. In *Internet and Distributed Computing Systems*, Giancarlo Fortino, Giuseppe Di Fatta, Wenfeng Li, Sergio Ochoa, Alfredo Cuzzocrea, and Mukaddim Pathan (Eds.). Springer, Cham, 437–446. DOI:https://doi.org/10.1007/978-3-319-11692-1_37

Robson de Oliveira Albuquerque, Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Rafael Timóteo de Sousa Júnior, and Tai-Hoon Kim. 2016. Leveraging information security and computational trust for cybersecurity. *J. Supercomput.* 72, 10 (Oct. 2016), 3729–3763. DOI:https://doi.org/10.1007/s11227-015-1543-4

Chrysanthos Dellarocas. 2000. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. In *Proceedings of the 2nd ACM Conference on Electronic Commerce (EC'00).* ACM Press, New York, New York, 150–157. DOI:https://doi.org/10.1145/352871.352889

Chrysanthos Dellarocas. 2003. The digitization of word of mouth: Promise and challenges of online feedback mechanisms. *Manage. Sci.* 49, 10 (Oct. 2003), 1407–1424. DOI:https://doi.org/10.1287/mnsc.49.10.1407.17308

Morton Deutsch. 1958. Trust and suspicion. *J. Conflict Resolut.* 2, 4 (Dec. 1958), 265–279. DOI:https://doi.org/10.1177/002200275800200401

Geetha D. Devanagavi, N. Nalini, and Rajashekhar C. Biradar. 2014. Trusted neighbors based secured routing scheme in wireless sensor networks using agents. *Wireless Personal Communications* 78, 1 (Sep. 2014), 1–28. DOI:https://doi.org/10.1007/s11277-014-1704-4

Valentin Dimitrov, Darius Palia, and Leo Tang. 2015. Impact of the Dodd-Frank act on credit ratings. *J. Financ. Econ.* 115, 3 (Mar. 2015), 505–520. DOI: https://doi.org/10.1016/j.jfineco.2014.10.012

eBay Inc. 2015. *eBay Annual Report.* Technical Report. eBay Inc. Retrieved from http://files.shareholder.com/downloads/ebay/2943142445x0x882672/742AC716-B4DB-40F8-83B0-793F0D6BDA5C/EBAY_2015_Annual_Report.pdf.

Passent El-Kafrawy, Emad Elabd, and Hanaa Fathi. 2015. A trustworthy reputation approach for web service discovery. *Procedia Comput. Sci.* 65 (2015), 572–581. DOI: https://doi.org/10.1016/j.procs.2015.09.001

Fabrício Enembreck and Jean-Paul André Barthès. 2013. A social approach for learning agents. *Expert Syst. Appl.* 40, 5 (Apr. 2013), 1902–1916. DOI: https://doi.org/10.1016/j.eswa.2012.10.008

Umar Farooq, Antoine Nongaillard, Yacine Ouzrout, and Muhammad Abdul Qadir. 2016a. A feature-based reputation model for product evaluation. *Int.J. Info. Technol. Decis. Mak.* 15, 6 (Nov. 2016), 1521–1553. DOI: https://doi.org/10.1142/S0219622016500358

Umar Farooq, Antoine Nongaillard, Yacine Ouzrout, and Muhammad Abdul Qadir. 2016b. A multi source product reputation model. *Comput. Industry* 83 (Dec. 2016), 55–67. DOI: https://doi.org/10.1016/j.compind.2016.08.002

Jochen Franke, Tim Stockheim, and Wolfgang König. 2005. The impact of reputation on supply chains. An analysis of permanent and discounted reputation. *Info. Syst. e-Bus. Manage.* 3, 4 (Dec. 2005), 323–341. DOI: https://doi.org/10.1007/s10257-005-0007-4

Jill Freyne, Lorcan Coyle, Barry Smyth, and Padraig Cunningham. 2010. Relative status of journal and conference publications in computer science. *Commun. ACM* 53, 11 (Nov. 2010), 124–132. DOI: https://doi.org/10.1145/1839676.1839701

Eric J. Friedman and Paul Resnick. 2001. The social cost of cheap pseudonyms. *J. Econ. Manage. Strategy* 10, 2 (June 2001), 173–199. DOI: https://doi.org/10.1111/j.1430-9134.2001.00173.x arxiv:1305.6836

Huafeng Gao, Peiyu Ren, Jun Wang, Yuyan Luo, and Wenqiang Tian. 2013. Study on reputation incentive effect of environmental pollution control in scenic area. *Int. J. Environ. Pollut.* 51, 3/4 (2013), 166–175. DOI: https://doi.org/10.1504/IJEP.2013.054027

David Giacomini and Anjali Agarwal. 2013. Optimizing end user QoS in heterogeneous network environments using reputation and prediction. *EURASIP J. Wireless Commun. Network.* 2013, 1 (Nov. 2013), 256–268. DOI: https://doi.org/10.1186/1687-1499-2013-256

Jones Granatyr, Vanderson Botelho, Otto Robert Lessing, Edson Emílio Scalabrin, Jean-Paul Barthès, and Fabrício Enembreck. 2015. Trust and reputation models for multiagent systems. *Comput. Surveys* 48, 2 (Oct. 2015), 1–42. DOI: https://doi.org/10.1145/2816826

Tyrone Grandison and Morris Sloman. 2000. A survey of trust in internet applications. *IEEE Commun. Surveys Tutor.* 3, 4 (2000), 1–30. DOI: https://doi.org/10.1109/COMST.2000.5340804

Marco Greco, Antonio Maurizio Branca, and Gianfranco Morena. 2011. An experimental study of the reputation mechanism in a business game. *Simul. Gam.* 42, 1 (Feb. 2011), 27–42. DOI: https://doi.org/10.1177/1046878110376793

Joe F. Hair Jr., Marko Sarstedt, Lucy M. Matthews, and Christian M. Ringle. 2016. Identifying and treating unobserved heterogeneity with FIMIX-PLS: Part I. *Eur. Bus. Rev.* 28, 1 (Jan. 2016), 63–76. DOI: https://doi.org/10.1108/EBR-09-2015-0094

Stephan Hammer, Michael Wißner, and Elisabeth André. 2015. Trust-based decision-making for smart and adaptive environments. *User Model. User-Adapt. Interact.* 25, 3 (Aug. 2015), 267–293. DOI: https://doi.org/10.1007/s11257-015-9160-8

Qiyi Han, Hong Wen, Mengyin Ren, Bin Wu, and Shengqiang Li. 2015. A topological potential weighted community-based recommendation trust model for P2P networks. *Peer-to-Peer Network. Appl.* 8, 6 (2015), 1048–1058.

Jonathan L. Herlocker, Joseph A. Konstan, Loren G. Terveen, and John T. Riedl. 2004. Evaluating collaborative filtering recommender systems. *ACM Trans. Info. Syst.* 22, 1 (Jan. 2004), 5–53. DOI: https://doi.org/10.1145/963770.963772 arxiv:50

Bruno W. P. Hoelz and Célia G. Ralha. 2015. Toward a cognitive meta-model for adaptive trust and reputation in open multi-agent systems. *Auton. Agents Multi-Agent Syst.* 29, 6 (Nov. 2015), 1125–1156. DOI: https://doi.org/10.1007/s10458-014-9278-9

Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. 2009. A survey of attack and defense techniques for reputation systems. *Comput. Surveys* 42, 1 (Dec. 2009), 1–31. DOI: https://doi.org/10.1145/1592451.1592452

Ian Horgan, Kamrul Ahsan, and Shah Miah. 2016. The importance of attributional trust to corporate reputation. *J. Relation. Market.* 15, 3 (jul 2016), 109–134. DOI: https://doi.org/10.1080/15332667.2016.1209045

V. Joseph Hotz and Juan Pantano. 2015. Strategic parenting, birth order, and school performance. *J. Pop. Econ.* 28, 4 (Oct. 2015), 911–936. DOI: https://doi.org/10.1007/s00148-015-0542-3

Daniel Houser and John Wooders. 2006. Reputation in auctions: Theory, and evidence from eBay. *J. Econ. Manage. Strat.* 15, 2 (June 2006), 353–369. DOI: https://doi.org/10.1111/j.1530-9134.2006.00103.x

Trung Dong Huynh, Nicholas R. Jennings, and Nigel R. Shadbolt. 2006. An integrated trust and reputation model for open multi-agent systems. *Auton. Agents Multi-Agent Syst.* 13, 2 (Sep. 2006), 119–154. DOI: https://doi.org/10.1007/s10458-005-6825-4

Saeed Javanmardi, Mohammad Shojafar, Shahdad Shariatmadari, and Sima S. Ahrabi. 2015. FR trust: A fuzzy reputation-based model for trust management in semantic P2P grids. *Int. J. Grid Util. Comput.* 6, 1 (2015), 57. DOI: https://doi.org/10.1504/IJGUC.2015.066397

David Jelenc and Denis Trček. 2014. Qualitative trust model with a configurable method to aggregate ordinal data. *Auton. Agents Multi-Agent Syst.* 28, 5 (2014), 805–835.

Li-Ming Jiang, Zhi-Ming Liu, Kun Zhang, Jian Xu, and Hong Zhang. 2015. Research on trust measure and management for open distributed systems based on dynamic grouping. *J. Commun.* 36 (2015). 10.11959/j.issn.1000-436x.2015012

Zhao Jiang, Zhou Xiaoguang, and Huang Meng Ni. 2016. Spontaneity geographic information reliability model based on user reputation. *J. Wuhan Univ. Info. Sci. Ed.* 41, 11 (2016), 1530–1536. DOI: https://doi.org/10.13203/j.whugis20140726

F.-S. Jin, M.-B. Dong, Z.-D. Niu, and Q.-X. Zhang. 2013. Reputation evaluation method for open multi-agent systems. *J. Beijing Inst. Technol. (English Ed.)* 22, 1 (2013), 75–80.

Audun Jøsang. 2007. Trust and reputation systems. In *Foundations of Security Analysis and Design IV*, Alessandro Aldini and Roberto Gorrieri (Eds.). Vol. 4677. Springer, Berlin, 209–245. DOI: https://doi.org/10.1007/978-3-540-74810-6_8

Audun Jøsang and Jochen Haller. 2007. Dirichlet reputation systems. In *Proceedings of the the 2nd International Conference on Availability, Reliability and Security (ARES'07)*. IEEE Computer Society, 112–119. DOI: https://doi.org/10.1109/ARES.2007.71

Audun Jøsang and Ross Hayward. 2006. Optimal trust network analysis with subjective logic. In *Proceedings of the 29th Australasian Computer Science Conference (ACSC'06)*, Vol. 48. Australian Computer Society, Inc., 85–94. DOI: http://dl.acm.org/citation.cfm?id=1151710

Audun Jøsang and Roslan Ismail. 2002. The beta reputation system. In *Proceedings of the 15th Bled Electronic Commerce Conference*. 2502–2511. Retrieved from http://aisel.aisnet.org/bled2002/41/.

Audun Jøsang, Roslan Ismail, and Colin Boyd. 2007. A survey of trust and reputation systems for online service provision. *Decision Support Systems* 43, 2 (Mar. 2007), 618–644. DOI: https://doi.org/10.1016/j.dss.2005.05.019

Nikolaus Kasimatis. 2015. *Papers in Economic Theory and the Biological Foundations of Economics.* Ph.D. Thesis. Simon Fraser University.

Sungwhan Kim. 2013. The effects of market structure and reputation on bankruptcy and banks performance. *Korean J. Financ. Eng.* 6 (2013), 139–160.

Anil Kini and Joobin Choobineh. 1998. Trust in electronic commerce: Definition and theoretical considerations. In *Proceedings of the 31st Hawaii International Conference on System Sciences*, Vol. 4. IEEE Computer Society, 51–61. DOI: https://doi.org/10.1109/HICSS.1998.655251

Barbara Kitchenham and Stuart Charters. 2007. *Guidelines for performing Systematic Literature Reviews in Software Engineering—Version 2.3.* EBSE Technical Report. Retrieved from https://pdfs.semanticscholar.org/e62d/bbbbe70cabcde3335765009e94ed2b9883d5.pdf.

Hichem Klabi, Sehl Mellouli, and Monia Rekik. 2016. A reputation based electronic government procurement model. *Govern. Info. Quart.* (Jan. 2016). DOI: https://doi.org/10.1016/j.giq.2016.01.001

Peter Kollock. 1999. The production of trust in online market. *Adv. Group Process.* 16, 1 (1999), 99–123. Retrieved from http://www.connectedaction.net/wp-content/uploads/2009/05/1999-peter-kollock-the-production-of-trust-in-online-markets.htm.

Andrew Koster. 2014. Trust and argumentation in multi-agent systems. *Argu. Comput.* 5, 2–3 (May 2014), 123–138. DOI: https://doi.org/10.1080/19462166.2014.885083

A. Koster, M. Schorlemmer, and J. Sabater-Mir. 2013. Opening the black box of trust: Reasoning about trust models in a BDI agent. *J. Logic Comput.* 23, 1 (Feb. 2013), 25–58. DOI: https://doi.org/10.1093/logcom/exs003

Simon Kramer, Rajeev Gore, and Eiji Okamoto. 2014. Computer-aided decision-making with trust relations and trust domains (cryptographic applications). *J. Logic Comput.* 24, 1 (Feb. 2014), 19–54. DOI: https://doi.org/10.1093/logcom/exs013

Kalliopi Kravari and Nick Bassiliades. 2016. DISARM: A social distributed agent reputation model based on defeasible logic. *J. Syst. Softw.* 117 (July 2016), 130–152. DOI: https://doi.org/10.1016/j.jss.2016.02.016

Mukesh Kumar and Kamlesh Dutta. 2016. LDAT: LFTM based data aggregation and transmission protocol for wireless sensor networks. *J. Trust Manage.* 3, 1 (Dec. 2016), 2. DOI: https://doi.org/10.1186/s40493-016-0023-y

Vikas Kumar and Prasann Pradhan. 2016. Reputation management through online feedbacks in e-business environment. *Int. J. Enter. Info. Syst.* 12, 1 (Jan. 2016), 21–37. DOI: https://doi.org/10.4018/IJEIS.2016010102

Nataliya Kussul and Ser Skakun. 2004. Neural network approach for user activity monitoring in computer networks. In *Proceedings of the International Joint Conference on Neural Networks (IJCNN'04)*, Vol. 2. IEEE. 1557–1561. DOI: https://doi.org/10.1109/IJCNN.2004.1380187

Nataliya Kussul and Serhiy Skakun. 2005. Intelligent system for users' activity monitoring in computer networks. In *Proceedings of the IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'05)*. IEEE, 306–309. DOI: https://doi.org/10.1109/IDAACS.2005.282992

Nataliia Kussul, Sergii Skakun, Andrii Yu. Shelestov, Olga Kussul, and Bohdan Yailymov. 2014. Resilience aspects in the sensor web infrastructure for natural disaster monitoring and risk assessment based on earth observation data. *IEEE J. Select. Topics Appl. Earth Observ. Remote Sens.* 7, 9 (Sep. 2014), 3826–3832. DOI: https://doi.org/10.1109/JSTARS.2014.2313573

Olga Kussul, Nataliia Kussul, and Sergii Skakun. 2013. Assessing security threat scenarios for utility-based reputation model in grids. *Comput. Secur.* 34 (May 2013), 1–15. DOI: https://doi.org/10.1016/j.cose.2013.01.006

Olga Kussul, Nataliia Kussul, and Sergii Skakun. 2015. A utility-based reputation model for grid resource management system. *Comput. Info.* 33, 5 (2015), 1139–1167.

Mohammed Laeequddin, B. S. Sahay, Vinita Sahay, and K. Abdul Waheed. 2010. Measuring trust in supply chain partners' relationships. *Measur. Bus. Excell.* 14, 3 (2010), 53–69. DOI: https://doi.org/10.1108/13683041011074218

Hady W. Lauw, Ee-Peng Lim, and Ke Wang. 2012. Quality and leniency in online collaborative rating systems. *ACM Trans. Web* 6, 1 (Mar. 2012), 1–27. DOI: https://doi.org/10.1145/2109205.2109209

John Lee and Neville Moray. 1992. Trust, control strategies and allocation of function in human-machine systems. *Ergonomics* 35, 10 (Oct. 1992), 1243–1270. DOI: https://doi.org/10.1080/00140139208967392

Jin Joo Lee, W. Bradley Knox, Jolie B. Wormwood, Cynthia Breazeal, and David DeSteno. 2013. Computationally modeling interpersonal trust. *Front. Psychol.* 4 (Dec. 2013), 1–14. DOI: https://doi.org/10.3389/fpsyg.2013.00893

Baichuan Li, Rong-Hua Li, Irwin King, Michael R Lyu, and Jeffrey Xu Yu. 2015. A topic-biased user reputation model in rating systems. *Knowl. Info. Syst.* 44, 3 (2015), 581–607.

Hui Lin, Jia Hu, Chuan Huang, Li Xu, and Bin Wu. 2015. Secure cooperative spectrum sensing and allocation in distributed cognitive radio networks. *Int. J. Distrib. Sensor Netw.* 11, 10 (Oct. 2015), 1–12. DOI: https://doi.org/10.1155/2015/674591

Greg Linden, Brent Smith, and Jeremy York. 2003. Amazon.com recommendations: Item-to-Item collaborative filtering. *IEEE Internet Comput.* 7, 1 (Jan. 2003), 76–80. DOI: https://doi.org/10.1109/MIC.2003.1167344 arxiv:69

Chang Liu, Yacine Ouzrout, Antoine Nongaillard, Abdelaziz Bouras, and JiLiu Zhou. 2014. Evaluation model for e-tourism product: A hidden Markov model-based algorithm. *Int. J. Technol. Manage.* 64, 1 (2014), 45. DOI: https://doi.org/10.1504/IJTM.2014.059235

Xin Liu, Anwitaman Datta, and Krzysztof Rzadca. 2013. Trust beyond reputation: A computational trust model based on stereotypes. *Electron. Commerce Res. Appl.* 12, 1 (2013), 24–39. DOI: https://doi.org/10.1016/j.elerap.2012.07.001 arxiv:1103.2215

Carlo Lodigiani and Michele Melchiori. 2016. A pagerank-based reputation model for VGI data. *Procedia Comput. Sci.* 98 (2016), 566–571. DOI: https://doi.org/10.1016/j.procs.2016.09.088

Gehao Lu, Joan Lu, Shaowen Yao, and Jim Yip. 2009. A review on computational trust models for multi-agent systems. *Open Info. Sci. J.* 2 (Mar. 2009), 18–25. DOI: https://doi.org/10.2174/1874947X00902020018

Kun Lu, Junlong Wang, and Mingchu Li. 2016. An eigentrust dynamic evolutionary model in P2P file-sharing systems. *Peer-to-Peer Network. Appl.* 9, 3 (2016), 599–612.

Yang K. Lu. 2013. Optimal policy with credibility concerns. *J. Econ. Theory* 148, 5 (Sep. 2013), 2007–2032. DOI: https://doi.org/10.1016/j.jet.2013.04.015

Manmeet Mahinderjit and Teo Yi. 2016. Hybrid multi-faceted computational trust model for online social network (OSN). *Int. J. Adv. Comput. Sci. Appl.* 7, 6 (2016). DOI: https://doi.org/10.14569/IJACSA.2016.070601

Elham Majd and Vimala Balakrishnan. 2015. Selecting advisor agents using reliability, reputation and risks. *J. Intell. Fuzzy Syst.* 29, 5 (June 2015), 1835–1846. DOI: https://doi.org/10.3233/IFS-151662

Stephen Paul Marsh. 1992. Trust and reliance in multi-agent systems: A preliminary report. In *Proceedings of the 4th European Workshop on Modeling Autonomous Agents in a Multi-Agent World (MAAMAW'92)*. Retrieved from https://www.researchgate.net/publication/2269307_Trust_and_Reliance_in_Multi-Agent_Systems_A_Preliminary_Report.

Stephen Paul Marsh. 1994. *Formalising Trust as a Computational Concept.* PhD Thesis. University of Stirling. Retrieved from http://www.cs.stir.ac.uk/research/publications/techreps/pdf/TR133.pdf.

Luis A. Martinez-Vaquero and José A. Cuesta. 2013. Evolutionary stability and resistance to cheating in an indirect reciprocity model based on reputation. *Phys. Rev. E* 87, 5 (May 2013), 052810. DOI: https://doi.org/10.1103/PhysRevE.87.052810

Hosein Marzi and Mengdu Li. 2013. An enhanced bio-inspired trust and reputation model for wireless sensor network. *Procedia Comput. Sci.* 19 (2013), 1159–1166. DOI: https://doi.org/10.1016/j.procs.2013.06.165

Lucy M. Matthews, Marko Sarstedt, Joseph F. Hair, and Christian M. Ringle. 2016. Identifying and treating unobserved heterogeneity with FIMIX-PLS. *Eur. Bus. Rev.* 28, 2 (Mar. 2016), 208–224. DOI: https://doi.org/10.1108/EBR-09-2015-0095

D. Harrison McKnight and Norman L. Chervany. 2001. Conceptualizing trust: A typology and e-commerce customer relationships model. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, Vol. 7. IEEE Computer Society. DOI: https://doi.org/10.1109/HICSS.2001.927053

Kevin McNally, Michael P. O'Mahony, and Barry Smyth. 2014. A comparative study of collaboration-based reputation models for social recommender systems. *User Model. User-Adapt. Interact.* 24, 3 (Aug. 2014), 219–260. DOI: https://doi.org/10.1007/s11257-013-9143-6

Fabrizio Messina, Giuseppe Pappalardo, Domenico Rosaci, Corrado Santoro, and Giuseppe M. L. Sarné. 2016. A trust-aware, self-organizing system for large-scale federations of utility computing infrastructures. *Future Gen. Comput. Syst.* 56 (2016), 77–94.

Ariel Monteserin and Analía Amandi. 2015. Whom should I persuade during a negotiation? An approach based on social influence maximization. *Decis. Supp. Syst.* 77 (Sep. 2015), 1–20. DOI:https://doi.org/10.1016/j.dss.2015.05.003

Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez. 2016. A model-driven approach for engineering trust and reputation into software services. *J. Netw. Comput. Appl.* 69 (July 2016), 134–151. DOI:https://doi.org/10.1016/j.jnca.2016.04.018

Lik Mui, Mojdeh Mohtashemi, and Ari Halberstadt. 2002a. A computational model of trust and reputation. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, Vol. 7. IEEE Computer Society, 188–196. DOI:https://doi.org/10.1109/HICSS.2002.994181

Lik Mui, Mojdeh Mohtashemi, and Ari Halberstadt. 2002b. Notions of reputation in multi-agents systems: A review. In *Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1 (AAMAS'02).* ACM Press, New York, New York, 280–287. DOI:https://doi.org/10.1145/544741.544807

Bonnie M. Muir. 1987. Trust between humans and machines, and the design of decision aids. *International J. Man-Machine Studies* 27, 5–6 (Nov. 1987), 527–539. DOI:https://doi.org/10.1016/S0020-7373(87)80013-5

Manh Hung Nguyen and Dinh Que Tran. 2013. A combination trust model for multi-agent systems. *Int. J. Innovat. Comput. Info. Control* 9, 6 (2013), 2405–2420.

Tung Doan Nguyen and Quan Bai. 2014. Accountable individual trust from group reputations in multi-agent systems. In *Trends in Artificial Intelligence*, Duc-Nghia Pham and Seong-Bae Park (Eds.). Springer, Cham, 1063–1075. DOI:https://doi.org/10.1007/978-3-319-13560-1_92

Mogens Nielsen. 2014. Trust in event structures. *Theoret. Comput. Sci.* 546 (Aug. 2014), 3–6. DOI:https://doi.org/10.1016/j.tcs.2014.02.039

Michael A. Nielsen and Isaac L. Chuang. 2011. *Quantum Computation and Quantum Information: 10th Anniversary Edition* (10th ed.). Cambridge University Press, New York, NY.

Manuel Gil Pérez, Félix Gómez Mármol, Gregorio Martínez Pérez, and Antonio F. Skarmeta Gómez. 2014. Building a reputation-based bootstrapping mechanism for newcomers in collaborative alert systems. *J. Comput. Syst. Sci.* 80, 3 (2014), 571–590.

Alexander M. Petersen, Santo Fortunato, Raj K. Pan, Kimmo Kaski, Orion Penner, Armando Rungi, Massimo Riccaboni, H. Eugene Stanley, and Fabio Pammolli. 2014. Reputation and impact in academic careers. *Proc. Natl. Acad. Sci. U.S.A.* 111, 43 (Oct. 2014), 15316–15321. DOI:https://doi.org/10.1073/pnas.1323111111 arxiv:1303.7274

Isaac Pinyol and Jordi Sabater-Mir. 2013a. Arguing about social evaluations: From theory to experimentation. *Int. J. Approx. Reason.* 54, 5 (July 2013), 667–689. DOI:https://doi.org/10.1016/j.ijar.2012.11.006

Isaac Pinyol and Jordi Sabater-Mir. 2013b. Computational trust and reputation models for open multi-agent systems: A review. *Artific. Intell. Rev.* 40, 1 (June 2013), 1–25. DOI:https://doi.org/10.1007/s10462-011-9277-z

Basit Qureshi, Geyong Min, and Demetres Kouvatsos. 2013. Countering the collusion attack with a multidimensional decentralized trust and reputation model in disconnected MANETs. *Multimedia Tools Appl.* 66, 2 (2013), 303–323.

Gurdeep Singh Ransi and Ziad Kobti. 2014. A hybrid artificial reputation model involving interaction trust, witness information and the trust model to calculate the trust value of service providers. *Axioms* 3, 1 (Feb. 2014), 50–63. DOI:https://doi.org/10.3390/axioms3010050

Paul Resnick, Neophytos Iacovou, Mitesh Suchak, Peter Bergstrom, and John Riedl. 1994. GroupLens: An open architecture for collaborative filtering of netnews. In *Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work (CSCW'94).* ACM Press, 175–186. DOI:https://doi.org/10.1145/192844.192905 arxiv:111

Paul Resnick and Richard Zeckhauser. 2002. Trust among strangers in internet transactions: Empirical analysis of eBay' s reputation system. In *The Economics of the Internet and E-commerce*, Michael R. Baye and John Maxwell (Eds.). Number 11 in Advances in Applied Microeconomics. Emerald Group Publishing Limited, 127–157. DOI:https://doi.org/10.1016/S0278-0984(02)11030-3 arxiv:arXiv:1011.1669v3

D. Rosaci and G. M. L. Sarné. 2013. Cloning mechanisms to improve agent performances. *J. Netw. Comput. Appl.* 36, 1 (Jan. 2013), 402–408. DOI:https://doi.org/10.1016/j.jnca.2012.04.018

Michael Rosemann and Wil van der Aalst. 2007. A configurable reference modelling language. *Info. Syst.* 32, 1 (Mar. 2007), 1–23. DOI:https://doi.org/10.1016/j.is.2005.05.003

Belén Ruiz, Águeda Esteban, and Santiago Gutiérrez. 2014. Determinants of reputation of leading spanish financial institutions among their customers in a context of economic crisis. *BRQ Bus. Res. Quart.* 17, 4 (Oct. 2014), 259–278. DOI:https://doi.org/10.1016/j.brq.2014.04.002

Sini Ruohomaa, Lea Kutvonen, and Eleni Koutrouli. 2007. Reputation management survey. In *Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES'07).* IEEE Computer Society, 103–111. DOI:https://doi.org/10.1109/ARES.2007.123

Pekka Ruotsalainen and Bernd Blobel. 2014. Trust information and privacy policies enablers for pHealth and ubiquitous health. In *Proceedings of the 11th International Conference on Wearable Micro and Nano Technologies for Personalized*

Health, Bernd Blobel, Stefan Sauermann, and Alexander Mense (Eds.). IOS Press, 133–139. DOI: https://doi.org/10.3233/978-1-61499-393-3-133

Pekka Sakari Ruotsalainen, Bernd Blobel, Antto Seppälä, and Pirkko Nykänen. 2013. Trust information-based privacy architecture for ubiquitous health. *JMIR mhealth uhealth* 1, 2 (Oct. 2013), 1–15. DOI: https://doi.org/10.2196/mhealth.2731

Jordi Sabater and Carles Sierra. 2005. Review on computational trust and reputation models. *Artific. Intell. Rev.* 24, 1 (2005), 33–60. DOI: https://doi.org/10.1007/s10462-004-0041-5

Antoine Salomon and Françoise Forges. 2015. Bayesian repeated games and reputation. *J. Econ. Theory* 159 (Sep. 2015), 70–104. DOI: https://doi.org/10.1016/j.jet.2015.05.014

Badrul Sarwar, George Karypis, Joseph Konstan, and John Reidl. 2001. Item-based collaborative filtering recommendation algorithms. In *Proceedings of the 10th International Conference on World Wide Web (WWW'01)*, Vol. 1. ACM Press, 285–295. DOI: https://doi.org/10.1145/371920.372071 arxiv:119

Vladimiro Sassone, Karl Krukow, and Mogens Nielsen. 2007. Toward a formal framework for computational trust. In *Formal Methods for Components and Objects*, Frank S. de Boer, Marcello M. Bonsangue, Susanne Graf, and Willem-Paul de Roever (Eds.). Vol. LNCS 4. Springer, Berlin, 175–184. DOI: https://doi.org/10.1007/978-3-540-74792-5_8

Emil Scarlat and Iulia Maries. 2011. Applying a computational trust and reputation model in communities of practice. *Rev. Econ. Studies Res. Virgil Madgearu* 4, 2 (2011), 59–77. Retrieved from https://www.ceeol.com/search/article-detail?id=49268.

Norbert Schwieters. 2015. A Magna Carta for the next industrial revolution. Retrieved from http://www.pwc.com/gx/en/issues/trust/redesigning-institutions.html.

Susan P. Shapiro. 1987. The social control of impersonal trust. *Amer. J. Sociol.* 93, 3 (Nov. 1987), 623–658. DOI: https://doi.org/10.1086/228791

Ye Eun Shin and EunKyoung Han. 2015. Why sponsor-event fit matters? *Korean J. Advert.* 26, 2 (2015), 241–260. Retrieved from http://www.earticle.net/article.aspx?sn=239563.

Surinder Singh, Vinod Kumar Verma, and Nagendra Prasad Pathak. 2015. Sensors augmentation influence over trust and reputation models realization for dense wireless sensor networks. *IEEE Sensors J.* 15, 11 (Nov. 2015), 6248–6254. DOI: https://doi.org/10.1109/JSEN.2015.2448642

Serhiy Skakun and Nataliya Kussul. 2006. An agent approach for providing security in distributed systems. In *Proceedings of the International Conference on Modern Problems of Radio Engineering, Telecommunications, and Computer Science (TCSET'06)*. IEEE, Lviv-Slavsko, Ukraine, 212–215. DOI: https://doi.org/10.1109/TCSET.2006.4404498

Sergey V. Skakun, Nataliya N. Kussul, and Alexander G. Lobunets. 2005. Implementation of the neural network model of users of computer systems on the basis of agent technology. *J. Auto. Info. Sci.* 37, 4 (2005), 11–18.

Boris Škorić, Sebastiaan J. A. de Hoogh, and Nicola Zannone. 2016. Flow-based reputation with uncertainty: Evidence-based subjective logic. *Int. J. Info. Secur.* 15, 4 (2016), 381–402.

Jose M. Such, Ana García-Fornes, Agustín Espinosa, and Joan Bellver. 2013. Magentix2: A privacy-enhancing agent platform. *Eng. Appl. Artific. Intell.* 26, 1 (Jan. 2013), 96–109. DOI: https://doi.org/10.1016/j.engappai.2012.06.009

Zeyu Sun, Longxing Li, and Xuelun Li. 2016. Research on intrusion detection technology based on nodes optimization deployment in wireless sensor networks. *Int. J. Secur. Appl.* 10, 8 (Aug. 2016), 159–172. DOI: https://doi.org/10.14257/ijsia.2016.10.8.14

Shoma Tanabe, Hideyuki Suzuki, and Naoki Masuda. 2013. Indirect reciprocity with trinary reputations. *J. Theor. Biol.* 317 (2013), 338–347. DOI: https://doi.org/10.1016/j.jtbi.2012.10.031 arxiv:1205.3547

W. T. Luke Teacy, Michael Luck, Alex Rogers, and Nicholas R. Jennings. 2012. An efficient and versatile approach to trust and reputation using hierarchical Bayesian modelling. *Artific. Intell.* 193 (Dec. 2012), 149–185. DOI: https://doi.org/10.1016/j.artint.2012.09.001

Thomson Reuters. 2014. WEB OF SCIENCE, Citation Report, Thomson Reuters. Retrieved from http://thomsonreuters.com/content/dam/openweb/documents/pdf/scholarly-scientific-research/fact-sheet/wos-next-gen-brochure.pdf.

Bo Tian, Jingti Han, and Kecheng Liu. 2016. Closed-loop feedback computation model of dynamical reputation based on the local trust evaluation in business-to-consumer E-commerce. *Information* 7, 1 (Feb. 2016), 4. DOI: https://doi.org/10.3390/info7010004

Ginés Dólera Tormo, Félix Gómez Mármol, and Gregorio Martínez Pérez. 2015. Dynamic and flexible selection of a reputation mechanism for heterogeneous environments. *Future Gen. Comput. Syst.* 49 (Aug. 2015), 113–124. DOI: https://doi.org/10.1016/j.future.2014.06.006

Denis Trček. 2014. Computational trust management, QAD, and its applications. *Informatica* 25, 1 (2014), 139–154. Retrieved from http://www.mii.lt/informatica/pdf/INFO895.pdf.

Gurkan Tuna, S. M. Potirakis, and G. Koulouras. 2013. Implementing a trust and reputation model for robotic sensor networks. *Elektron. Elektrotech.* 19, 10 (2013), 3–8.

Joana Urbano, Ana Paula Rocha, and Eugénio Oliveira. 2011. A dynamic agents' behavior model for computational trust. In *Proceedings of the 15th Portuguese Conference on Artificial Intelligence: Progress in Artificial Intelligence (EPIA'11)*, Luis Antunes and H. Sofia Pinto (Eds.). Springer, Berlin, 536–550. DOI: https://doi.org/10.1007/978-3-642-24769-9_39

Joana Urbano, Ana Paula Rocha, and Eugénio Oliveira. 2014. An approach to computational social trust. *AI Commun.* 27, 2 (2014), 113–131. DOI:https://doi.org/10.3233/AIC-130587

Moshe Y. Vardi. 2009. Conferences vs. journals in computing research. *Commun. ACM* 52, 5 (May 2009), 5. DOI:https://doi.org/10.1145/1506409.1506410

Veronica Venturini, Javier Carbo, and Jose. M. Molina. 2013. CALoR: Context-aware and location reputation model in AmI environments. *J. Ambient Intell. Smart Environ.* 5, 6 (2013), 589–604. DOI:https://doi.org/10.3233/AIS-130231

Vinod Kumar Verma, Surinder Singh, and N. P. Pathak. 2016. Impact of malicious servers over trust and reputation models in wireless sensor networks. *Int. J. Electron.* 103, 3 (Mar. 2016), 530–540. DOI:https://doi.org/10.1080/00207217.2015.1036803

Omar Abdel Wahab, Jamal Bentahar, Hadi Otrok, and Azzam Mourad. 2015. A survey on trust and reputation models for Web services: Single, composite, and communities. *Decis. Support Syst.* 74 (June 2015), 121–134. DOI:https://doi.org/10.1016/j.dss.2015.04.009

Fei Wang, Fu Rong Wang, Benxiong Huang, and Laurence T. Yang. 2013. ADVS: A reputation-based model on filtering SPIT over P2P-VoIP networks. *J. Supercomput.* 64, 3 (2013), 744–761. DOI:https://doi.org/10.1007/s11227-010-0545-5

Jin Wang, Yonghui Zhang, Youyuan Wang, and Xiang Gu. 2016. RPRep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETs. *Int. J. Distrib. Sensor Netw.* 2016, 3 (2016), 1–15. DOI:https://doi.org/10.1155/2016/6138251

Jane Webster and Richard T. Watson. 2002. Analyzing the past to prepare for the future: Writing a literature review. *MIS Quart.* 26, 2 (2002), xiii–xxiii. Retrieved from https://web.njit.edu/~egan/Writing_A_Literature_Review.pdf.

Zhe Wei and Fang Wang. 2014. Negative multinomial reputation for self-organized networks. *New Gen. Comput.* 32, 1 (Jan. 2014), 9–29. DOI:https://doi.org/10.1007/s00354-014-0101-6

Andrew G. West. 2013. *Damage detection and mitigation in open collaboration applications.* Dissertation. University of Pennsylvania. Retrieved from https://repository.upenn.edu/cgi/viewcontent.cgi?article=1974&context=edissertations.

Adam Wierzbicki, Tomasz Kaszuba, Radoslaw Nielek, Paulina Adamska, and Anwitaman Datta. 2013. Improving computational trust representation based on Internet auction traces. *Decis. Support Syst.* 54, 2 (2013), 929–940. DOI:https://doi.org/10.1016/j.dss.2012.09.016

Quanwang Wu, Qingsheng Zhu, and Peng Li. 2015. A neural network based reputation bootstrapping approach for service selection. *Enterpr. Info. Syst.* 9, 7 (Oct 2015), 768–784. DOI:https://doi.org/10.1080/17517575.2013.845913

Li Xu and Hongwei Yu. 2013. Multi-dimension reputation model design in multi-agent system. *J. Tongji Uni.* (2013). Retrieved from http://en.cnki.com.cn/Article_en/CJFDTOTAL-TJDZ201303026.htm.

Xiao Ya, Zheng Shihui, and Sun Bin. 2015. Trusted GPSR protocol without reputation faking in VANET. *J. China Uni. Posts Telecommun.* 22, 5 (Oct. 2015), 22–55. DOI:https://doi.org/10.1016/S1005-8885(15)60676-8

Su-Rong Yan, Xiao-Lin Zheng, Yan Wang, William Wei Song, and Wen-Yu Zhang. 2015. A graph-based comprehensive reputation model: Exploiting the social context of opinions to enhance trust in social commerce. *Info. Sci.* 318 (Oct. 2015), 51–72. DOI:https://doi.org/10.1016/j.ins.2014.09.036

Han Yu, Zhiqi Shen, Cyril Leung, Chunyan Miao, and Victor R. Lesser. 2013. A survey of multi-agent trust management systems. *IEEE Access* 1 (Jan. 2013), 35–50. DOI:https://doi.org/10.1109/ACCESS.2013.2259892

Han Yu, Zhiqi Shen, Chunyan Miao, Bo An, and Cyril Leung. 2014c. Filtering trust opinions through reinforcement learning. *Decis. Supp. Syst.* 66 (2014), 102–113.

Ruiyun Yu, Rui Liu, Xingwei Wang, and Jiannong Cao. 2014a. Improving data quality with an accumulated reputation model in participatory sensing systems. *Sensors* 14, 3 (Mar. 2014), 5573–5594. DOI:https://doi.org/10.3390/s140305573

Yao Yu, Zhaolong Ning, and Lei Guo. 2016. A secure routing scheme based on social network analysis in wireless mesh networks. *Sci. China Info. Sci.* 59, 12 (Dec. 2016). DOI:https://doi.org/10.1007/s11432-015-5467-7

Yao Yu, Yuhuai Peng, Yinpeng Yu, and Tianyu Rao. 2014b. A new dynamic hierarchical reputation evaluation scheme for hybrid wireless mesh networks. *Comput. Electric. Eng.* 40, 2 (Feb. 2014), 663–672. DOI:https://doi.org/10.1016/j.compeleceng.2013.05.005

Giorgos Zacharia, Alexandros Moukas, and Pattie Maes. 1999. Collaborative reputation mechanisms in electronic marketplaces. In *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences (HICSS'99)*, Vol. 00. IEEE Comput. Soc, 7. DOI:https://doi.org/10.1109/HICSS.1999.773057

Mariem Zekri, Badii Jouaber, and Djamal Zeghlache. 2010. On the use of network QoS reputation for vertical handover decision making. In *Proceedings of the IEEE Globecom 2010 Workshop on Advances in Communications and Networks.* IEEE, 2006–2011. DOI:https://doi.org/10.1109/GLOCOMW.2010.5700296

Kan Zhang and Nick Antonopoulos. 2013. A novel bartering exchange ring based incentive mechanism for peer-to-peer systems. *Future Gen. Comput. Syst.* 29, 1 (Jan. 2013), 361–369. DOI:https://doi.org/10.1016/j.future.2011.06.005

Yuhui Zhong, Bharat Bhargava, Yi Lu, and Pelin Angin. 2015. A computational dynamic trust model for user authorization. *IEEE Trans. Depend. Secure Comput.* 12, 1 (Jan. 2015), 1–15. DOI:https://doi.org/10.1109/TDSC.2014.2309126

Ling Zhu and Jie Lin. 2016. Optimal merchandise selection strategy in e-store promotional webpage. *J. Electron. Commerce Org.* 14, 2 (Apr. 2016), 1–15. DOI: https://doi.org/10.4018/JECO.2016040101

Roie Zivan, Harel Yedidsion, Steven Okamoto, Robin Glinton, and Katia Sycara. 2015. Distributed constraint optimization for teams of mobile sensing agents. *Auton. Agents Multi-Agent Syst.* 29, 3 (May 2015), 495–536. DOI: https://doi.org/10.1007/s10458-014-9255-3

Received January 2017; revised April 2018; accepted June 2018