Information Sciences 333 (2016) 88–107

Contents lists available at ScienceDirect

Information Sciences

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

An interval type-2 fuzzy logic based framework for reputation management in Peer-to-Peer e-commerce

Giovanni Acampora [a,*], Daniyal Alghazzawi [b], Hani Hagras [c], Autilia Vitiello [d]

[a] School of Science and Technology, Nottingham Trent University, NG8 11NS Nottingham, UK
[b] Faculty of Computing and Information Technology, King AbdulAziz University, P.O. Box 13154, Jeddah, Saudi Arabia
[c] School of Computer Science and Electronic Engineering, University of Essex, CO4 3SQ Colchester, UK
[d] Department of Computer Science, University of Salerno, Fisciano, Salerno 84084, Italy

ARTICLE INFO

Article history:
Received 5 May 2015
Revised 19 September 2015
Accepted 11 November 2015
Available online 17 November 2015

Keywords:
Type-2 fuzzy sets
E-commerce
Trust management
Reputation management systems

ABSTRACT

During the last two decades, the Internet has changed people's habits and improved their daily life activities and services. In particular, the emergence of e-commerce provided manufactures and vendors with more business opportunities. This allowed customers to benefit from a global, quicker and cheaper shopping environment. However, e-commerce is evolving from a centralised approach, where consumers directly purchase products and services from businesses, to a Peer-to-Peer (P2P) perspective, in which customers buy and sell goods amongst themselves. In P2P scenarios, it is crucial to protect both buyers and sellers (the peers) from being victimised by possible fraud arising from the uncertainties, vagueness and ambiguities that characterise the interactions amongst unknown business entities. For this reason, the so-called reputation models are becoming a key architectural component of any e-commerce portal. These systems are intended to evaluate the basic features of each entity (buyer, seller, goods, etc.) involved in a given trading transaction in order to assess the trust level of the given transaction and minimise fraud. However, in spite of their wide deployment, the reputation models need to be enhanced to handle the various sources of uncertainties in order to produce more accurate outputs which will allow to increase the trust and decrease the fraud levels within e-commerce systems. In this paper, we present an interval type-2 fuzzy logic based framework for reputation management in (P2P) e-commerce which is capable of better handling the faced uncertainties. We have carried out various experiments based on eBay®-like transaction datasets which have shown that the proposed type-2 fuzzy logic based system can provide better performance (in terms of malicious peer detection and exchanged message overhead) when compared to the other well-known and heavily used approaches like the eBay® approach, EigenTrust, PeerTrust as well as the type-1 fuzzy based counterpart approach.

1. Introduction

The Internet and the *World Wide Web* (WWW) improved the lifestyle of people from all over the World in different aspects of everyday life activities and services. Thanks to mobile network technologies, people can now get access from anywhere and at

* Corresponding author. Tel.: +44 1158488348; fax: +44 7851919903.
E-mail addresses: giovanni.acampora@ntu.ac.uk, gianni.acampora@gmail.com (G. Acampora), danielg@kau.edu.su (D. Alghazzawi), hani@essex.ac.uk (H. Hagras), avitiello@unisa.it (A. Vitiello).

http://dx.doi.org/10.1016/j.ins.2015.11.015
0020-0255/

any time to a set of increasing social and economic services enabling a smart and quick exploitation of resources and facilities. One of the most important and fast growing Internet based sectors is *e-commerce* which started around 1991 when the Internet was opened to commercial use. Since that date, numerous businesses were launched on websites which employed transaction automation to improve the efficiency and reliability. E-commerce is completely changing the way in which people, customers and/or vendors, perform their negotiations and exchange goods and services. E-commerce can be seen as defining a new "economy" by providing more business opportunities to manufactures and companies. In addition, e-commerce allows customers to benefit from a quicker and cheaper shopping on the Internet.

E-commerce started by following the *Business to Consumer* (B2C) paradigm [1] where consumers purchase products and services directly from businesses. This paradigm represents a sort of marketplace for the worldwide exposure of products. In this centralised paradigm, customers are protected from eventual frauds since the quality of the sale service depends only upon the *reputation* of the seller company that acts as an authority to mediate transaction flows.

The recent years are witnessing the evolution of a new e-commerce paradigm called *Peer-to-Peer (P2P)* or *Consumer to Consumer (C2C)* [1] in which customers buy and sell among themselves without using a centralised e-commerce authority. The extensive development of this new business paradigm is due to the reduction in costs. Indeed, sellers can post their goods over the Internet cheaply compared to the high rent space in a store and, as a consequence, they can sell with lower prices by producing a financial gain for buyers. However, in such a new business context, it is crucial to protect both buyers and sellers (peers) from being victimised by possible frauds due to the uncertainties, vagueness and ambiguities which characterise the interactions amongst unknown business entities. For this reason, the so-called reputation models aimed at assessing the trust levels of peers during trade transactions are becoming a key architectural component of any e-commerce portal.

The main goal of reputation models is to compute and associate a reputation value to each peer by using the community-based opinions in order to allow buyers/sellers to undertake more reliable transactions. Three core components are used to build any reputation system: (1) the trust value that each peer has for another peer involved in at least one transaction with it; (2) the distribution method that propagates these values in the P2P network; (3) the reputation score that each peer aggregates from the trust values gathered from all the peers interacting with it [2]. The quality of a reputation-based P2P trust management system is depending on its capability in performing an accurate and effective identification of malicious peers, and in efficiently reducing the bandwidth usage of the P2P network.

Due to the importance of their role in enabling safety in P2P e-commerce paradigm, there has been a fervent development of such systems. In particular, after some first attempts to model reputation concepts as crisp values, recently, the uncertain and imprecise nature of commercial transactions opened the way for promising applications of fuzzy logic theory to this important research area (see Section 2). Nevertheless, the precise identification of malicious peers and the consequent improvement of safety in trade transactions is far from being completely solved.

In this paper, we aim at bridging this gap by introducing a collection of e-commerce trustworthiness metrics starting from which to design an innovative reputation model and its implementation based on the type-2 fuzzy sets theory [3–5]. Different from conventional Mamdani or TSK type-1 fuzzy systems, type-2 fuzzy sets provide additional design degrees of freedom, which can achieve better performance in domains where lots of uncertainties are present [6], such as P2P e-commerce environments. Indeed, thanks to its capability to handle high level of uncertainty, the proposed framework is capable of performing a deep and precise analysis of all the different parameters involved in a given trading transaction and assessing the right reputation value for each peer belonging to a P2P e-commerce system.

We have carried out various experiments based on eBay®-like transaction datasets to compare, in an empirical and statistical way, the proposed system with other well-known and widely used approaches, such as the eBay® paradigm (used in the most known e-market platform eBay®), EigenTrust and PeerTrust (which are two of the most cited reputation management systems in P2P environments), as well as, a type-1 fuzzy based approach. As shown by these comparisons, the proposed type-2 fuzzy logic based system yields better performance than state-of-the-art approaches in terms of malicious peer detection and exchanged message overhead.

The rest of the paper is organised as follows: Section 2 reports a detailed description of the state-of-the-art about the reputation management systems; Section 3 will present the background knowledge including an overview on the reputation management issues in P2P e-commerce systems and a brief description of type-2 FLSs; Section 4 presents the proposed interval type-2 fuzzy logic based framework for reputation management; Section 5 presents the experiments and results while Section 6 presents the conclusions and future work.

2. Related works

Reputation management systems play a crucial role in allowing the existence and efficiency of e-commerce thanks to their capability to defend sellers and customers from on-line frauds. In literature, several paradigms have been proposed with the goal to provide on-line community with even more efficient reputation management systems. The eBay® reputation-based P2P trust management system is the most popular trust-management system and it is a based a user feedback approach [7] that enables eBay® users to evaluate the reputation value of their trading peers, and store these values to a centralised reputation database.

EigenTrust [8] is one of the most widely accepted paradigms for reputation management in distributed environments. EigenTrust paradigm computes the trust score by summing the satisfactions of the transaction with each peer and then normalises it over all its peers [8]. Then, it calculates the reputation value of a peer by aggregating the trust values assigned to it by other peers, weighted by the reputations of the assigning peers. The trust scores are distributed in the P2P network by using a Distributed

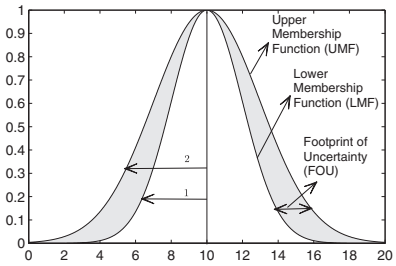

Fig. 1. An interval type-2 fuzzy set.

Hash Table (DHT)-overlay network [9]. In [10], the PeerTrust paradigm was presented to overcome the drawbacks of EigenTrust in controlling the man-in-the-middle attack [11] as it uses overlay for trust propagation and public-key infrastructure for securing remote scores. In addition, the PeerTrust was the first to introduce the concept of feedback creditability to aggregate the global reputation.

The above mentioned paradigms have mainly employed crisp logic which cannot easily handle the different uncertainties, vagueness and ambiguities that characterise the interactions occurring amongst unknown business entities in P2P systems (for more details see Section 3.2). Type-1 fuzzy logic was employed to develop a first fuzzy based reputation system, namely FuzzyTrust [12]. FuzzyTrust works by performing two inference steps: (1) trust score calculation where each peer performs a fuzzy inference on local parameters to generate trust scores towards the other peers and (2) reputation aggregation where each peer performs a weighted aggregation of the trust scores received from all peers to produce a reputation value. The propagation of trust scores is executed by using a Distributed Hash Table (DHT)-overlay network with an architecture similar to that of Chord [13]. As shown by a comparison in terms of malicious peer detection, FuzzyTrust outperforms EigenTrust in malicious peer identification, albeit slightly. In spite of good results provided by FuzzyTrust, it cannot easily handle and model the uncertainties present in P2P e-commerce as they employ crisp and precise type-1 fuzzy sets [14] (i.e. their Membership Functions (MFs) are supposedly known perfectly) which does not allow for any uncertainties about membership values. As better described in the next section, interval type-2 fuzzy sets [15,16] are characterised by fuzzy membership functions which provide additional degrees of freedom that make it possible to directly model and handle the strong uncertainties present in P2P e-commerce.

Starting from this consideration, our proposal is aimed at improving the performance of the state-of-the-art reputation systems in e-commerce context, by exploiting the recognised superiority of type-2 FS in modelling knowledge and processing uncertain information. In the next section, we provide more details about type-2 fuzzy logic and reputation management issues in order to show how the type-2 fuzzy logic can better face reputation management issues with respect to the state-of-the-art approaches.

3. Background knowledge

This section is devoted to provide a background knowledge of the concepts related to interval type-2 fuzzy logic systems, reputation management in P2P e-commerce and how type-2 fuzzy logic can face reputation management issues.

3.1. Brief overview of the interval type-2 fuzzy logic systems

Fuzzy set theory was first introduced by Zadeh [17] and has been accepted over years as a methodology for building systems that can deliver satisfactory performance in the face of uncertainty and imprecision [18,19]. However, the same Zadeh [15], recognised that Type-1 Fuzzy Sets (T1 FSs) are able to partially handle the concept of uncertainty, whereas real-world applications are often characterised by multiple sources of strong uncertainty, ambiguity and vagueness [14]. As a consequence, recent years have shown a significant attention in research toward more suitable forms of fuzzy logic [18], such as the Interval Type-2 Fuzzy Sets (IT2 FSs) shown in Fig. 1. IT2 FSs are considered to be potentially more appropriate in modelling uncertainty, thanks to their capability of providing extra degrees of freedom [18]. This capability is due to the exploitation of a new type of *fuzzy membership function* where the membership value, for each element of the universe of the discourse, is a type-1 fuzzy set and not a crisp value. The use of IT2 FSs to represent the inputs and/or outputs of a Fuzzy Logic System (FLS) leads to the so-called Interval Type-2 Fuzzy Logic Systems (IT2FLSs) (shown in Fig. 2).

In detail, an IT2 FLS works as follows [14,20]: the crisp inputs are first fuzzified into input type-2 fuzzy sets; singleton fuzzification is usually used in interval type-2 FLS applications due to its simplicity and suitability for embedded processors and real time applications. The input type-2 fuzzy sets then activate the inference engine and the rule base to produce output type-2 fuzzy sets. The type-2 FLS rule base remains the same as for the type-1 FLS but its Membership Functions (MFs) are represented by interval type-2 fuzzy sets instead of type-1 fuzzy sets. The inference engine combines the fired rules and gives a mapping from input type-2 fuzzy sets to output type-2 fuzzy sets. The type-2 fuzzy output sets of the inference engine are then processed by the type-reducer which leads to type-1 fuzzy sets called the type-reduced sets. There are different types of type-reduction methods. In this paper we use the centre of sets type-reduction as it has a reasonable computational complexity that lies between

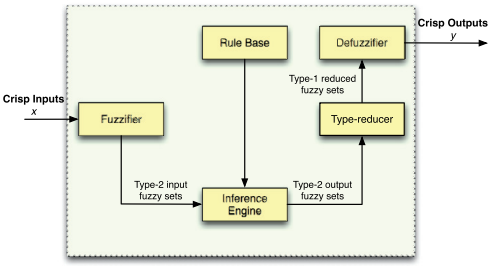

Fig. 2. Structure of a type-2 FLS.

the computationally expensive centroid type-reduction and the simple height and modified height type-reductions which have problems when only one rule fires [14,20]. After the type-reduction process, the type-reduced sets are defuzzified (by taking the average of the type-reduced set) so as to obtain crisp outputs. More information regarding the interval type-2 FLS can be found in [14].

Due to their capability to handle with high level of uncertainty, IT2 FLSs have been successfully implemented in many real world applications, including intelligent control [21], time series predictions [22,23], pattern recognition [24], image processing [25], medical diagnosis [26], collision avoidance of autonomous vehicles [27] and many others. In the next section, we show how benefits of the IT2 FLSs can be exploited to address reputation management issues in P2P e-commerce.

3.2. Reputation management issues in P2P e-commerce systems

In Peer-to-Peer (P2P) systems, peers are both consumers and providers of services. Given that there is no authority to dictate the rules for peer interaction and that interactions often occur among previously unknown parties, peers might maliciously behave and harm others in the system [28]. Therefore, one of the fundamental challenges for the development of open and decentralised P2P systems, is the ability to manage risks that may arise when interacting and collaborating with previously unknown and potentially malicious peers. This challenge, is even more felt in P2P e-commerce systems, where the interaction between unknown parties involves business interests, and, as a consequence of a malicious behaviour, there may be an economic loss or even a fraud. As an example, a malicious buyer may not provide a payment for a received good, whereas, a malicious seller may not send goods which has been paid for.

As proved in [29–31], in P2P systems, peers with the capability of reasoning about *trust* can potentially mitigate the risks caused by malicious behaviours. Hence, the so-called *trust management systems* play a crucial role in enabling trading with untrustworthy peers in e-commerce scenarios [32]. The conventional trust management systems [33] are based on access control credentials, i.e., they foresee that peers use credential verification to enable access control to restricted services. Our research work focuses on *reputation-based trust management systems* where service requesters select the relative providers based on their reputation values. This choice is due to the wide applicability of the reputation-based trust management systems to P2P environment where the credential based conventional methods cannot be used because of their dependence to a centralised credential authority [34]. In literature, various definitions have been given for the related but distinct concepts of reputation and trust. One definition of "trust" was cited in [35], where it is considered as *"a subjective expectation a partner has about another future behaviour based on the history of their encounters"*. This definition treats the trust as a subjective property computed based on the two partners involved in a dyadic encounter. In e-commerce, the partners are peers and an encounter is a trade transaction between them. As for the reputation concept, we consider the definition given by the *Concise Oxford English Dictionary* [36], which agrees with the social network researcher's point of view [37], which states: *"the reputation is what is generally said or believed about a person's or thing's character or standing"*. Therefore, in our context, the reputation is the collected and processed information about one former peer's behaviour, as experienced by all the other ones within the system. Starting from these trust and reputation definitions, it is easy to note that the main tasks of a reputation-based trust management system for a P2P e-commerce environment are enabling peers to rate each other with a trust value, after the completion of a trade transaction and to aggregate these values for a given partner to derive its relative global reputation score. In this scenario, where a peer gives an opinion towards the other ones, another important concept emerges called *credibility* which can be defined as *"the expectation that a rating peer has the capability and the willingness to provide a correct opinion towards the other ones"* [38].

As a result of this discussion, P2P systems for e-commerce need to deal with high levels of uncertainties, vagueness and ambiguities which include:

- absence of an authority to dictate the rules for peer interaction and to avoid peers maliciously behave and harm others in the system;
- trading transactions occur among unknown parties potentially acting in a malicious way;
- use of the reputation value as a credibility score (examples of reputation systems which follow this strategy are EigenTrust [8] and FuzzyTrust [12]). This strategy is not sufficiently accurate, since some peers could behave well sending high quality

goods (in the case they are sellers) or quick payment (in the case they are buyers) and at the same time, provide inaccurate or false opinions;
- supply of good trading services by a peer for a while in order to build a good reputation. Then, suddenly, the peer starts cheating buyers or sellers by exploiting that reputation.

Due to lots of uncertainties above mentioned, type-2 fuzzy logic results to be the most suitable methodology to efficiently deal with trust, reputation and credibility concepts. For this reason, we propose a new reputation management system based on IT2 FLSs. Indeed, as described above, IT2 FSs provide additional degrees of freedom which can handle the high level of uncertainties present in P2P e-commerce environments and provide a more suitable representation of peers' dynamic characteristics. As shown in the experiment section, the exploitation of IT2 FLSs to face reputation management system issues will result in better performance (in terms of malicious peer detection and exchanged message overhead) when compared to the fuzzy and non fuzzy counterparts. Before giving all details about experiments, in the next section, the proposed system is presented in all its components.

4. The proposed type-2 fuzzy logic based reputation management framework for P2P e-commerce

This section introduces a type-2 fuzzy logic based reputation management framework which uses a new reputation model defining a set of formal metrics for evaluating the concepts of reputation, trust and credibility in uncertain environments. The framework is arranged in a hierarchical structure of IT2 FLSs. All membership functions and rules of the designed IT2 FLSs are based on subjective opinions from different reputation experts who casted their personal beliefs about trustworthiness in e-commerce. This design strategy is particularly suitable in P2P e-commerce environments where the methods for learning fuzzy membership functions and rules (e.g. genetic algorithms, particle swarm optimisation and so on) are hard to be applied due to the challenge in assembling the training data sets. Precisely, the strong dynamic features characterising P2P e-commerce such as (1) the dynamic behaviour of peers in performing trading transactions, and (2) the fast changes occurring in a P2P network in terms of the number of the peers and relationships among them, make it hard to identify a training dataset which is sufficiently informative and not tied to particular and limited situations. As a consequence, the exploitation of these misleading datasets could lead the conventional learning methods to produce unrealistic rules which violate the e-commerce rules. As an example, automatic learning approaches based on static datasets might not be able to identify evolving malicious peer behaviours such as the oscillatory behaviours consisting in building a good reputation by making a series of transactions involving cheap goods and trying to make a profit through expensive fraudulent transactions. Our framework bridges this gap by introducing a new reputation model taking into account temporal information and its evaluation by means of a type-2 architecture.

Hereafter, firstly, we present the new model defining a set of formal metrics for evaluating the concepts of reputation, trust and credibility in uncertain environments and, then, we describe the architecture of the proposed type-2 fuzzy logic based reputation management system and all its components.

4.1. New model for reputation management in P2P e-commerce

This section introduces an innovative model for reputation management in P2P e-commerce environments. Inspired by the general P2P reputation model presented in [28] and by eBay® vision on feedback concept[1], the proposed model is aimed at providing trust and reputation computation with a set of well-defined metrics and dynamic features that will enable the next generation of reputation management frameworks to achieve improved performance in terms of accuracy of malicious peer identification. Due these innovative metrics, the proposed model provides reputation management frameworks with adequate reaction functionalities to address quick changes in peers' behaviour avoiding malicious situations where peer could provide good trading services for a while, building a good reputation, and then suddenly start cheating buyers or sellers by exploiting that reputation. As a consequence, this approach will enable a more efficient identification of very sly malicious peers such as the hypocritical and oscillatory ones (see Section 5.2).

In order to achieve these goals, the proposed model for reputation management in P2P e-commerce focuses on three main principles:

1. trust and reputation evolve over time being sensitive to new experiences;
2. the sensitivity to new experiences should not be dependent on old ones;
3. the past experiences should not be ignored.

The first principle means that trust and reputation do not decay over time if there are no new experiences, i.e., trade transactions. Hence, positive experiences may lead to an increase of trust and reputation value, while negative ones may decrease such values.

The sensitivity of trust and reputation values to new experiences is essential to capture the changes in peers behaviour. Indeed, even if a peer has shown a trustworthy behaviour for a period of time, it should still be possible to detect and decrease its reputation if it suddenly starts exhibiting malicious behaviour [28]. In order to enforce this principle, it is necessary to provide the independence of this sensitivity to new experiences from the old ones (second principle). In our model, this leads to consider three kinds of trust denoted as *Transaction Trust*, *Historical Trust* and *Overall Trust* (see Table 1). In order to keep the independence

[1] http://pages.ebay.com/help/feedback/allaboutfeedback.html .

Table 1
Definitions of different kinds of the trust.

Trust typology	Definition
Transaction Trust	The trust that a peer has towards another one by considering only the newest transaction that occurred between them.
Historical Trust	The trust that a peer has towards another one before the last transaction between them.
Overall Trust	The trust computed by a peer towards another one by considering all transactions that occurred between them.

Table 2
Metrics influencing transaction trust.

Metric	Definition
Metrics used by a buyer	
Goods Quality	The quality assessed by the buyer about the received goods.
Delivery Time	The amount of time required to receive goods.
Seller Communication Quality	The quality assessed by the buyer about the seller's readiness and availability at communicating.
Shipping Service Reliability	The objective reliability provided through the shipping service used by the seller.
Metrics used by a seller	
Payment Time	The amount of the time required to receive buyer's payment
Payment Method Reliability	The objective reliability provided by the payment method used by the buyer.
Buyer Communication Quality	The quality assessed by the seller about the buyer's readiness and availability at communicating.

Table 3
Factors influencing the overall trust.

Metric	Definition
Historical Trust Date	It represents the date when the historical trust value was computed. This factor allows to discriminate between new and old experiences and to give more relevance to the transaction trust.
Last Transaction Amount	It represents the price of the goods involved in the last transaction between two peers. This factor supports the detection of oscillatory behaviours (i.e. behaviours characterised by a lot of honest and cheap transactions and a few malicious and expensive ones).

of new experiences from old ones, the proposed model computes the transaction trust by only considering metrics that do not depend upon trading transactions occurred in the past. In particular, the used metrics are inspired from eBay® vision and differs according to the role of peers (sellers or buyers). The complete list is reported in Table 2.

However, even if new experiences are considered more important than the old ones since they represent the current behaviour of a peer, past experiences cannot be ignored at all (third principle). Indeed, old experiences can be used to re-establish peer trustworthiness after recovering from an intrusion attack which affected its reputation [28]. Moreover, the consideration of past experiences is relevant to detect possible peer oscillatory behaviours consisting in building a good reputation by making a series of transactions involving cheap goods and, consecutively, trying to make a profit through expensive fraudulent transactions. Due to the relevance of past experiences, as aforementioned, the proposed model considers the so-called historical trust. In detail, the proposed model expects a peer to compute the overall trust value towards another one by aggregating historical and transaction trusts. This aggregation takes into account the factors reported in Table 3.

Apart from discussing the trust concepts, the proposed model defines also which factors are involved in the reputation computation. In detail, a peer computes its own reputation by means of the aggregation of overall trusts received by other peers involved in transactions with it. For sake of simplicity, from now on, we will denote as *target peer*, the one which takes care of computing its own reputation, and as *commentator peer*, the one which sends its opinion (overall trust value) over a target peer which was involved in a transaction with it[2]. Like for trust concept, the computation of the reputation considers the new experiences more important than old ones. As a consequence, overall trusts received in more recent period have more weight in the reputation aggregation step. Moreover, since multiple interactions between peers allow a more accurate evaluation, also overall trusts computed on a greater number of transactions have more weight in the aggregation step. Finally, in order to support the detection of oscillatory behaviours, the reputation aggregation is influenced by average amount of goods involved in the transactions between the target peer and commentator ones. However, the factor which mostly affects the reputation aggregation step is the credibility of commentator peers. By concluding, in the reputation aggregation step, each weight associated with a received overall trust is influenced by the metrics reported in Table 4.

As described in the next section, the defined model for reputation management in e-commerce scenarios has been implemented in a reputation management system based on a type-2 fuzzy sets-based architecture. In particular, we focus on this

[2] It is important to point out that such distinction is made only for the ease of exposition, since a peer may act simultaneously both as target and as commentator.

Table 4
Factors influencing weights associated to the overall trust.

Metric	Definition
Credibility	The willingness of the commentator peer to provide a correct opinion towards the target one.
Opinion Date	The date when the commentator user computed the overall trust value for the target one.
Opinion Scope	The number of transactions on which the commentator user computed the overall trust value for the target one.
Average Amount	The average price of goods involved in the transactions, on which the commentator user computed the overall trust value for the target one.

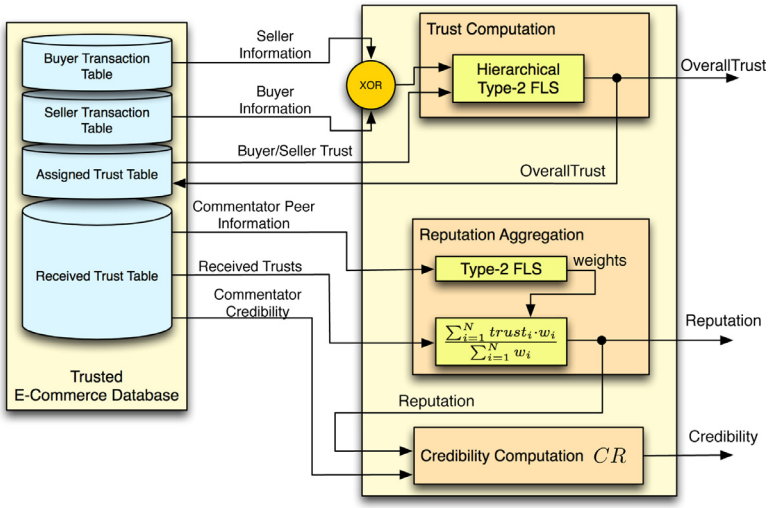

Fig. 3. The architecture of the proposed reputation management system.

emergent fuzzy theory, since type-2 fuzzy sets may succeed to model the uncertain and imprecise nature of trust and reputation concepts by imitating human reasoning more efficiently than type-1 fuzzy sets.

4.2. The interval type-2 fuzzy architecture for reputation management

The proposed interval type-2 fuzzy system for reputation management works by using a hierarchical and incremental approach where the values related to trust concepts, defined by the aforementioned model, are computed in order to aggregate a final reputation value for each peer involved in trading transactions. In particular, a transaction trust value is computed after a trading transaction is completed between two peers $P1$ and $P2$, to enable $P1$ to assess how good was the behaviour of $P2$ in that transaction, and vice versa. $P1$, then computes an overall trust, T_{12}, to assess how good was the behaviour of $P2$ in all trading transactions made with $P2$. In the same way $P2$ computes an overall trust value, T_{21}, to assess how good was the behaviour of $P1$ in past transactions made with $P2$. Finally, $P1$ sends the value T_{12} to $P2$ in order to enable $P2$ to aggregate this value with other overall trust values coming from other peers to finally compute its reputation. By the same way, $P2$ sends T_{21} to $P1$. In order to make the aggregation step more reliable, our architecture uses a novel credibility concept to assure the authenticity of information exchanged by peers. In order to perform all the aforementioned computations, each peer is equipped with the type-2 fuzzy architecture shown in Fig. 3 which is composed of the following modules: *Trust Computation Module*, *Reputation Aggregation Module*, *Credibility Computation Module* and *Trusted E-commerce Database*.

The *Trust Computation Subsystem* is used by a peer (acting as commentator peer) to evaluate the level of trustiness over another one (in this case acting as target peer) with whom it has just closed a trade transaction. It is implemented through a hierarchical Interval Type-2 Fuzzy Logic Systems (IT2FLSs) which computes, at the low level, the transaction trust value and, at the top level, the overall trust value over the peer with whom it has just closed the transaction.

The *Reputation Aggregation Subsystem* is used by a target peer to compute its own reputation (representing the final output of the proposed type-2 fuzzy set based reputation management framework). In order to compute such value, a target peer performs a weighted aggregation of overall trust values received by peers which have been involved in at least a transaction with it. The weights used in the computation are calculated through an IT2 FLS. Once computed a real value representing own reputation, the target peer is classified malicious if this value is labelled with the linguistic term *Low* of the fuzzy variable *Reputation* (see Fig. 5(g)).

The *Credibility Computation Module* is used by a target peer to update the credibility value of all its commentator peers (peers which have been involved in at least a transaction with it and have sent it their overall trust values over it). This updating is always performed after a transaction between the target peer and any commentator peer. The credibility value for a commentator peer is

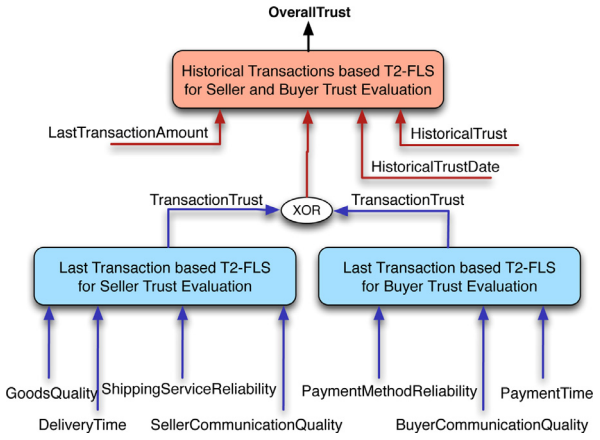

Fig. 4. The hierarchical type-2 fuzzy system composing the trust computation subsystem.

based on the reputation value of the target peer just computed. In detail, the credibility value of a commentator peer is increased if its opinion (overall trust value) over the target peer is near to the new computed reputation for the target peer, decreased vice versa.

The *Trusted E-commerce Database* is used to locally store a set of data necessary for the computations performed by the other modules. In short, these data are closed in four tables: *buyer transaction table* contains data related to transactions where the peer acts as buyer; *seller transaction table* contains data related to transactions where the peer acts as seller; *assigned trust table* contains data related to overall trust values computed over the other peers; *received trust value* contains data related to overall trust values received by the other peers.

Hereafter, more details about the architecture modules and the interactions among them are given.

4.2.1. Trust Computation Subsystem

The Trust Computation Subsystem is used by a peer (acting as commentator peer) to evaluate the level of trustiness over another one (in this case acting as target peer) with whom it has just closed a trade transaction. Such subsystem is implemented through a hierarchical IT2FLSs which computes the trust values according to the above mentioned e-commerce trust model. The hierarchical IT2FLSs is composed of two levels (see Fig. 4): the lower one is used to compute the trust value over the target peer by considering only information related to the last transaction occurred with it (the transaction trust), whereas, the top one is used to refine the trust value computed by the lower layer by using a set of information related to all transactions made with the target peer (the overall trust).

The lower level uses different information, depending on whether the commentator peer is evaluating a target peer that has acted as seller or buyer in the last transaction. According to the proposed e-commerce reputation model, when the target peer acts as seller, the lower level IT2FLS will have four input variables, named *Goods Quality*, *Deliverity Time*, *Seller Communication Quality* and *Shipping Service Reliability* and an output one named *Transaction Trust*. The input variables reflect the metrics used by a buyer reported in the Table 2.

The rule base[3] of the lower IT2FLS for a seller peer is composed from 108 rules which were inspired by the paradigm where the higher the quality of goods and the shorter the delivery time and the higher the seller communication quality and the higher the shipping service reliability, the higher is the value of the transaction trust. When the target peer acts as buyer in the last transaction, the lower layer IT2FLS will have different inputs (reflecting the metrics used by a seller reported in the Table 2) which are *Payment Time*, *Buyer Communication Quality* and *Payment Method Reliability*. The rule base[4] of the lower IT2FLS for a buyer peer is composed of 36 rules which were inspired by the paradigm where the higher the buyer communication quality and the higher the payment method reliability and the shorter the payment time, the higher is the value of the transaction trust.

The top level IT2FLS of the hierarchical type-2 FLS has four input variables named *Last Transaction Amount*, *Transaction Trust*, *Historical Trust* and *Historical Trust Date*, and one output variable representing the overall trust denoted by the variable *Overall Trust*. In detail, the variables *Last Transaction Amount* and *Historical Trust Date* reflects the metrics reported in the Table 3, whereas, the variable *Transaction Trust* represents the output of the lower level of the designed hierarchical type-2 fuzzy system. Finally, the variable *Historical Trust* represents the trust value calculated by the commentator peer over the target one before the last transaction occurred. The rule base[5] of the top level IT2FLC is composed from 225 rules which were inspired by the paradigms: (1) the higher the amount of the last transaction, the higher is the importance of the transaction trust value; (2) the newer the date of the historical trust and the higher is the importance of the historical trust value.

[3] http://old.di.unisa.it/dottorandi/avitiello/research/Type-2FuzzyControllerXBuyerTrust.xlsx .
[4] http://old.di.unisa.it/dottorandi/avitiello/research/Type-2FuzzyControllerXSellerTrust.xlsx .
[5] http://old.di.unisa.it/dottorandi/avitiello/research/Type-2FuzzyControllerXTopTrust.xlsx .

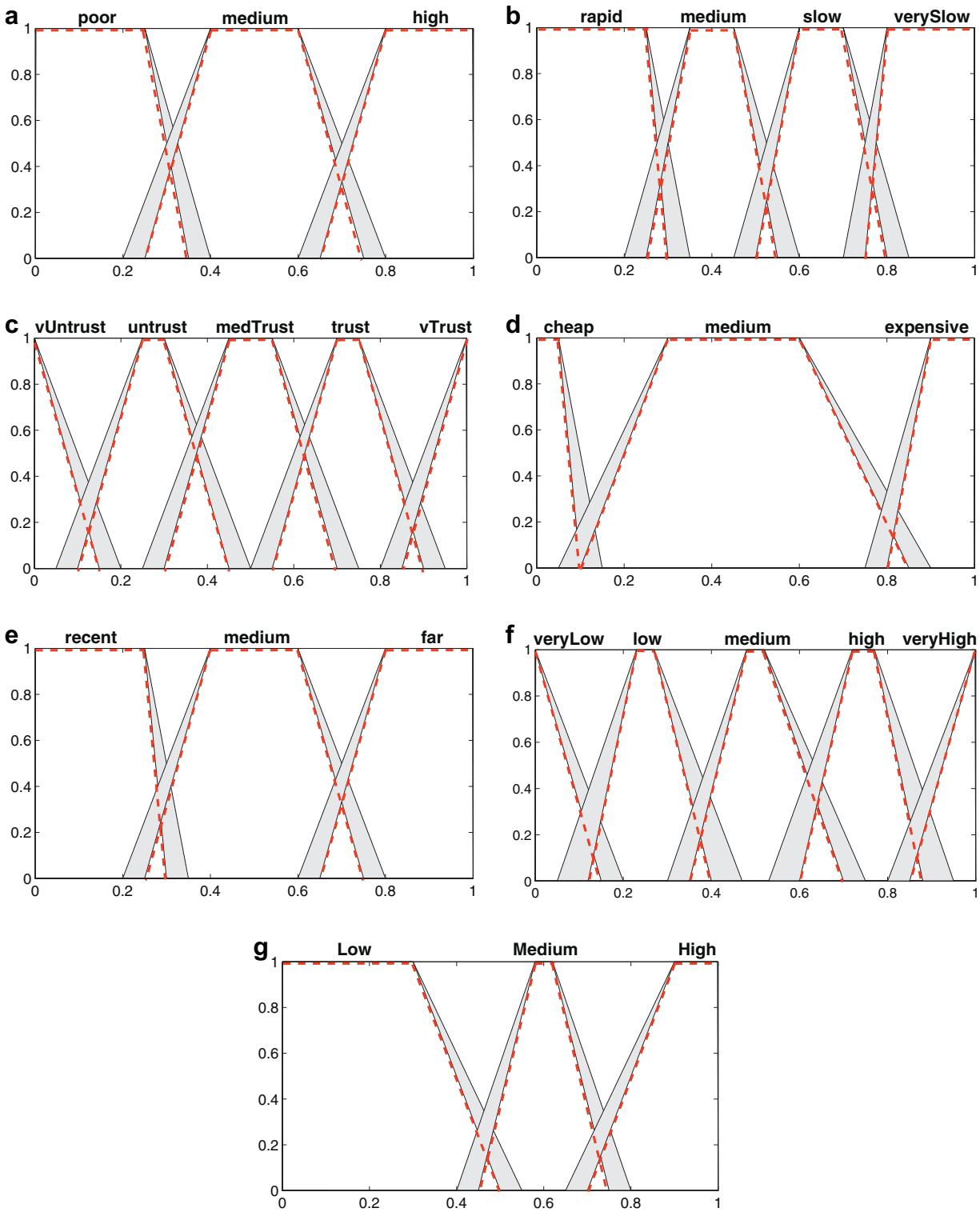

Fig. 5. (a) Type-2 fuzzy sets for the variables *Goods Quality*, *Seller Communication Quality*, *Shipping Service Reliability*, *Buyer Communication Quality*, *Payment Method Reliability*, *Credibility* and *Opinion Scope*; (b) Type-2 fuzzy sets for the variables *Deliverity Time* and *Payment Time*; (c) Type-2 fuzzy sets for the variables *Transaction Trust*, *Historical Trust* and *Overall Trust*; (d) Type-2 fuzzy sets for the variables *Last Transaction Amount* and *Average Amount*; (e) Type-2 fuzzy sets for the variables *Historical Trust Date* and *Opinion Date*; (f) Type-2 fuzzy sets for the variable *Weight*; (g) Fuzzy sets for the linguistic variable *Reputation*. The dotted lines represent the shape of type-1 fuzzy sets used in experimental results section. See http://old.di.unisa.it/dottorandi/avitiello/research/Type-2FuzzyVariables.xlsx for the numeric parameters of the type-2 membership functions.

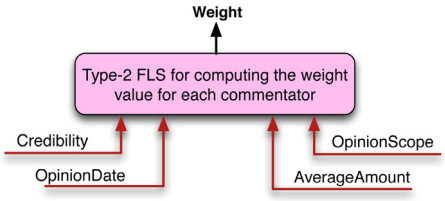

Fig. 6. The IT2FLS aimed at computing the weight for each commentator peer.

All of type-2 FS memberships of the designed hierarchical IT2 FLS are displayed in Fig. 5. All of type-2 FS memberships and the related FOUs have been designed by means of a strong interaction with some experts in the field of security in P2P systems which allowed us to perfectly tune our reputation system in order to strongly overcome the performance of current systems. In particular, all of type-2 FS memberships have been modelled by means of trapezoidal fuzzy sets because this shape is more suitable for representing the expert knowledge provided in terms of a collection of intervals. As for inference engine details, all the IT2FLSs used in this paper use *min* operator for implication, *min–max* operator for composition, the centre of sets type-reduction [39] and the defuzzification is obtained by taking the average of the type-reduced sets produced from type-reduction [40].

4.2.2. Reputation Aggregation Subsystem

The Reputation Aggregation Subsystem is used by a peer to compute its own reputation value which is a real number within the interval [0,1], where 1 represents the highest reputation value. In order to compute such value, a target peer considers the overall trust values provided by all the peers which have been involved in a transaction with it. In particular, this subsystem is composed of three components where the first component is devoted to performing a weighted aggregation of received trust values, the second component is aimed at computing a weight for each received trust value and the third component is introduced to support a semantic interpretation of the computed reputation value. The first module calculates the reputation value R through the following formula:

$$R = \frac{\sum_{i=1}^{N} trust_i * w_i}{\sum_{i=1}^{N} w_i} \tag{1}$$

where N is the number of commentator peers which have completed a transaction with the target peer, both with the role of buyer and seller; $trust_i$ is the overall trust value computed over the target peer by the commentator one i; and finally, w_i is the weight representing how much the target peer weights the overall trust value $trust_i$ provided by the ith commentator peer. In order to compute the values w_i, a target peer uses the second module of the reputation aggregation subsystem which is an IT2FLS (shown in Fig. 6). According to the metrics reported in the Table 4, this IT2FLS has four input variables, which are *Credibility*, *Opinion Date*, *Opinion Scope*, *Average Amount*, and returns the output weight (represented by the variable *Weight*). Fig. 5(a) shows type-2 fuzzy sets for the variables *Credibility* and *Opinion Scope*, whereas, Figs. 5(d) and (e) show, respectively, type-2 fuzzy sets for the variable *Average Amount* and the variable *Opinion Date*. The interval type-2 fuzzy sets representing the output variable *Weight* are displayed in Fig. 5(f). In this IT2FLS, the rule base[6] is composed of 81 rules inspired from paradigm where the higher the credibility and the newer the date and the higher the number of involved transactions and the higher the average amount, the higher is the value of the weight.

Once a reputation value is computed, characterising what is a good/bad reputation is non trivial [41]. The third component of the aggregation reputation subsystem is aimed at accomplishing this task through the exploitation of a linguistic variable, named *Reputation* (see Fig. 5(g)), defined by expert knowledge. In detail, the third component of the aggregation reputation subsystem is devoted to fuzzify the real reputation value computed by the first component of the same subsystem in order to determine the badness of peer behaviours. In particular, the proposed system considers a peer as malicious when it is labelled with the *Low* linguistic term.

4.2.3. Credibility Computation Subsystem

The Credibility Computation Subsystem is used by a target peer to update the credibility value of all the other peers which have been involved in at least a transaction with it. Many reputation systems (e.g. EigenTrust [8], FuzzyTrust [12]) use the reputation value as a credibility one. However, this strategy is not sufficiently accurate, since some peers could behave well sending high quality goods, in the case they are sellers, or quick payment, in the case they are buyers, and, at the same time, provide inaccurate or false opinions. Therefore, we consider each peer characterised by reputation and credibility values as concepts disjointed between them.

In the proposed system, the target peer performs the updating of credibility of commentator peers after each transaction, by considering its new reputation value according to the approach presented in [42]. Initially, each peer which joins the network is assigned a neutral credibility value of 0.5 (the range of credibility value is [0, 1]). Then, such value of credibility is increased or

[6] http://old.di.unisa.it/dottorandi/avitiello/research/Type-2FuzzyControllerXCommentatorWeight.xlsx .

decreased depending on the accuracy of its own opinion (overall trust value) over a target peer. More precisely, the credibility value is increased if the degree of closeness between the given opinion and the new computed reputation for the target peer lies within a tolerance value ϵ, otherwise it is decreased. Formally, this subsystem computes the *Credibility Value* (*CR*) as shown in Eq. (2):

$$CR = \begin{cases} CR_{old} + Inc \cdot e^{-2 \cdot error} \cdot \frac{1}{1+(10 \cdot (CR_{old}-0,5))^2} & \text{if } |error| \leq \epsilon \\ CR_{old} - Dec \cdot CR_{old}^4 & \text{if } |error| > \epsilon \end{cases} \quad (2)$$

where CR_{old} is the current credibility value of the peer, *error* is the difference between the given opinion and the new computed reputation, ϵ is the tolerance value, *Inc* is the maximal possible increment and *Dec* is the maximal possible decrement. In particular, in the proposed system, we set *Inc* to 0.05 and *Dec* to 0.2. The choice to set $Dec > Inc$ is derived from human perception, according to which it is harder to gain credibility than to loose it [43]. As for the variable ϵ, it is set to 0.3 because such value causes a peer to move between two different trust levels (represented by fuzzy sets in Fig. 5(c)). Therefore, the system we propose tolerates an error which does not lead to a change in the overall trust level of a peer. After computing the new credibility value for all the commentator peers, the target peer sends these values to the corresponding ones which store them.

4.2.4. Trusted E-commerce Database

The information used by the Trust Computation Module, the Reputation Aggregation Module and the Credibility Computation Module are stored into four tables held by each peer. In detail, they are:

- the *buyer transaction table* which contains information about transactions where the peer was the buyer. Therefore, this table contains a record for each transaction where the peer buys a good. In particular, the fields named Delivery Time, Shipping Service Reliability, Seller Communication Quality and Goods Quality are used as input to the lower IT2FLS used for seller evaluation in the Trust Computation Module, whereas, the field Amount is used as input for the top IT2FLS of the Trust Computation Module;
- the *seller transaction table* which contains information about transaction where the peer was the seller. Therefore, this table contains a record for each transaction where the peer sells a good. In particular, the fields named Payment Time, Payment Method Reliability and Buyer Communication Quality are used as input to the lower IT2FLS used for buyer evaluation in the the Trust Computation Module, whereas, the field Amount is used as input for the top IT2FLS of the Trust Computation Module;
- the *assigned trust table* which contains information about trust values computed over the other peers. Therefore, this table contains a record for each peer with which one has been involved in a transaction. In particular, the fields named Trust value and Date are used as input for the top IT2FLS of the Trust Computation Module, respectively, for the variables Historical Trust and Historical Trust Date. Moreover, the fields named Trust value and Date are updated after the execution of the Trust Computation Module. In detail, the value of the Trust field is updated with the overall trust value, instead, the value of the Date field is updated with the date of the executed computation;
- the *received trust table* which contains information about the overall trust received by the commentator peers. Therefore, this table contains a record for each peer with which one has been involved in a transaction. In particular, the fields named Credibility, Opinion Date, Opinion Scope and Average Amount are used as input to the IT2FLS of the Reputation Aggregation Module in order to compute weights for commentator peers, whereas, the values of the field Trust value are the overall trust values used in the Eq. (1). It is worth noting that all information contained in a record of this table does not change until the execution of a new transaction with the commentator peer belonging to the record, except for the credibility value, which is sent by each commentator peer after each transaction involving the target peer.

Table 5 reports the description of each field contained in these tables in a detailed way. Moreover, each peer keeps track of its own reputation value and its own credibility.

4.2.5. The proposed type-2 fuzzy logic based reputation system at work

In this section, we analyse the functioning of the proposed reputation management system after a transaction between a seller *S* and a buyer *B*. For sake of exposition simplicity, let us consider *S* as the target peer and the set $\Phi(S) = \{P_1, P_2, \ldots, P_n\}$, with $n = |\Phi(S)|$, as the group of the peers which have been involved in at least a transaction with *S*. Therefore, each peer $C \in \Phi(S)$ and the buyer *B* act as commentator peers. The task of computation of the reputation value for target peer *S*, involves the activities shown in Fig. 7. The same mechanism affects the peer *B* after the performed transaction with the peer *S* by assuming the role of "target peer". By analysing the message overhead, after each transaction, the number of exchanged messages is the sum of the number of exchanged messages by peers *S* and *B* which is strongly influenced by the number of peers belonging to the set Φ (different for the peers *A* and *B*).

A comparison of the proposed reputation management system with the state-of-the-art approaches in terms of exchanged messages is reported in the next section, after an evaluation of the proposed reputation management system in terms of detection rate of the malicious peers.

5. Experiments and results

In this section, we will report various experiments which were conducted to illustrate the benefits of the proposed system in detecting malicious peers and reducing the usage of bandwidth in P2P networks. We have compared the performance yielded by

Table 5
Scheme of tables stored by each peer.

Field name	Description
Buyer transaction table	
Id Transaction	Identifier of the transaction
Seller	Peer providing the goods
Amount	Price of the goods
Delivery Time	Time which has been needed to receive the goods
Shipping Service Reliability	Reliability of the used shipping service
Seller Communication Quality	Availability at communicating of the peer providing the goods
Goods Quality	Quality of the purchased goods
Seller transaction table	
Id Transaction	Identifier of the transaction
Buyer	Peer who buys the goods
Amount	Price of the goods
Payment Time	Time which has been necessary to receive the payment
Payment Method Reliability	Reliability of the used payment method
Buyer Communication Quality	Availability at communicating of the peer buying the goods
Assigned trust table	
Peer	Peer receiving the trust value
Trust value	The given opinion over the peer
Date	Date in which the trust value has been computed and sent to the peer
Received trust table	
Peer	Commentator peer providing the trust value
Credibility	Credibility value of the peer providing the trust value
Trust value	The received opinion
Opinion Date	Date in which the trust value has been received
Opinion Scope	Number of transactions performed with the peer
Average Amount	Average price of the goods involved in the transactions performed with the peer

the proposed system with state-of-the-art paradigms, including: (1) the reputation management system used by the most known e-market P2P platform, eBay®, (2) one of the most cited reputation management systems in P2P environments, EigenTrust [8], (3) one of the most cited reputation management systems in e-commerce P2P environments, PeerTrust [10], and (4) a version of the proposed reputation system based on conventional type-1 fuzzy sets. In the carried out experiments, the compared systems are executed in a simulated P2P environment based on Intel® Core™ i5-2410M, 2.3 GHz CPU and 4 GB of RAM.

In the following section, we will present the datasets used to perform the planned experimental sessions. Section 5.2 shows the effectiveness of our proposal by highlighting and reporting its capability of detecting malicious peers in terms of absolute precision and recall. Section 5.3 reports comparisons between the proposed system and the state-of-the-art reputation management systems; these comparisons have been conducted in terms of percentage of detected malicious peers, number of frauds occurred in a simulated scenario based on eBay® auctions, and message overhead.

5.1. The employed datasets

In spite of the large number of research activities accomplished in the reputation management area, no consolidated and public datasets are available to perform unified and replicable experiments. As a consequence, a large dataset has been created by downloading real eBay® transactions from eBay® databases through the eBay® SDK[7]. This dataset contains the last 100 transactions performed by each of the sellers belonging to a specific Italian category of goods, i.e., the data storage devices. This dataset is composed of about 5000 transactions, occurring in the period from February to July 2013, whereas, the number of peers (including sellers and buyers) is 4503. In order to evaluate the proposed system in different situations involving a different number of peers, we built three new datasets, referred to as *dataset1*, *dataset2* and *dataset3*, which respectively include the 10%, 50% and 100% of transactions contained in the original dataset. Therefore, these new datasets are, respectively, composed of 490, 2307 and 4503 peers. We have augmented *dataset1*, *dataset2* and *dataset3* with different percentages of malicious peers involved in different malicious transactions. As described in [44], malicious peers are those that both misbehave and lie in providing their feedbacks values. In particular, in our context, malicious peers misbehave by making, as buyers, late or no payments, and, as sellers, delivering bad-quality goods or not delivering them at all [12]. In literature, the most studied malicious behaviours are known as *Naive*, *Discriminatory*, *Hypocritical* and *Oscillatory* [45] which can be explained as follows:

- *Naive*: the malicious peer always misbehaves and gives unfairly low recommendations about the others [46];
- *Discriminatory*: the malicious peer selects a group of victims and always misbehaves with them [8,46]. Besides, it gives unfairly low recommendations about victims. For other peers, it behaves as a good one;

[7] https://go.developer.ebay.com/ .

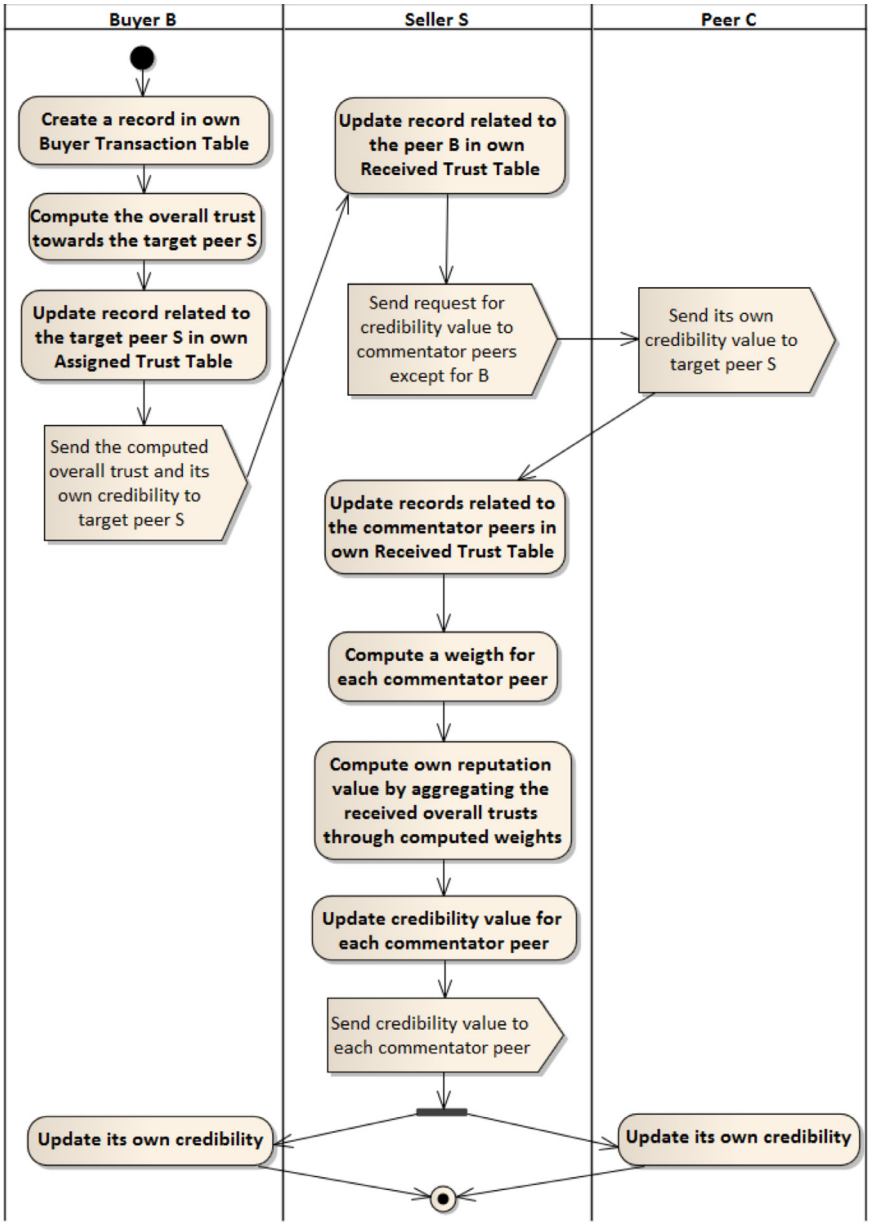

Fig. 7. The activity diagram related to the reputation computation by the seller *S* after a transaction with the buyer *B*.

- *Hypocritical*: the malicious peer misbehaves and gives unfairly low recommendation with x percent probability [8,47]. In other times, it behaves as a good peer;
- *Oscillatory*: the malicious peer builds its own high reputation by being good for a long time period, during which, it performs transactions characterised by small amounts of money. Then, it behaves as a naive peer for a short period of time by performing transactions characterised by large amounts of money. After the malicious period, it becomes a good peer again.

Each artificial malicious transaction involves a good peer, already present in the original dataset, with a synthetic malicious peer. The new datasets are named *MaliciousDataset_X_Y*, where $X = 1, 2, 3$ represents the starting dataset, i.e, *dataset1*, *dataset2* or *dataset3*, and $Y = 5, 10, 20$ is the percentage of added malicious peers, i.e, 5%, 10% and 20%. The number of synthetic Naive, Discriminatory, Hypocritical and Oscillatory peers within each dataset is the same. In particular, by considering malicious peer definition, Hypocritical peers have been created by considering x equal to 25%, 50%, or 75%, Discriminatory buyers have been created by considering as victims the 10% of all sellers, whereas, Discriminatory sellers select only 1% of all buyers as victims. Table 6 shows the details of the number of peers involved in all planned experimental sessions.

Hereafter, the details about the performed experiments are given.

Table 6
Number of peers characterising the datasets used by all planned experimental sessions.

Dataset	Number of peers
MaliciousDataset_1_5	514
MaliciousDataset_1_10	538
MaliciousDataset_1_20	587
MaliciousDataset_2_5	2411
MaliciousDataset_2_10	2537
MaliciousDataset_2_20	2768
MaliciousDataset_3_5	4727
MaliciousDataset_3_10	4952
MaliciousDataset_3_20	5403

Table 7
$Precision_{malicious}$ and $Recall_{malicious}$ of the proposed reputation system.

Dataset	$Precision_{malicious}$	$Recall_{malicious}$
MaliciousDataset_1_5	0.82	0.92
MaliciousDataset_1_10	0.81	0.88
MaliciousDataset_1_20	0.82	0.88
MaliciousDataset_2_5	0.99	0.83
MaliciousDataset_2_10	0.88	0.86
MaliciousDataset_2_20	0.89	0.85
MaliciousDataset_3_5	0.89	0.84
MaliciousDataset_3_10	0.89	0.84
MaliciousDataset_3_20	0.87	0.87
Average	0.87	0.86

5.2. Evaluation of the proposed reputation management system

In this section, we analyse the capability of the proposed reputation management system in detecting malicious peers. As described in Section 4.2.2, our system considers a peer as malicious when it is characterised by a reputation value labelled with the *Low* linguistic term. The performance of our system is measured through the use of two well-established metrics, namely *Precision* and *Recall*. Precisely, in reputation scenario, precision and recall are defined as follows:

$$Precision_{malicious} = \frac{tp}{tp + fp} \tag{3}$$

$$Recall_{malicious} = \frac{tp}{tp + fn} \tag{4}$$

where *tp* is the number of *true positives*, i.e., the number of malicious peers which are correctly identified as malicious, *fp* is the number of *false positives*, i.e., the number of good peers that are identified as malicious, and *fn* is the number of the *false negatives*, i.e., the number of malicious peers that are wrongly identified as good peers. The values *tp*, *fp* and *fn* have been computed by applying the proposed reputation management system to a dataset of trading transactions performed in a past interval time in order to label each peer, involved in those transactions, as malicious or not malicious; successively, for each peer, the label computed by the reputation management system (malicious, not malicious) is compared with the real nature of the same peer (malicious, not malicious) in the original dataset. The result of these comparisons determines the value of *tp*, *fp* and *fn*.

Table 7 shows the $Precision_{malicious}$ and $Recall_{malicious}$ values obtained by the proposed reputation management system by considering all created malicious datasets. Table 8 shows the detection rate (which is computed using the $Recall_{malicious}$) in percentage for each kind of malicious peer by considering the same nine datasets.

As shown in the Table 7, the proposed system yields good performance, being characterised by an average $Precision_{malicious}$ equals to 0.87 and an average $Recall_{malicious}$ equals to 0.86.

5.3. Comparative study with the state-of-the-art paradigms

In this section, we compare of the proposed system with EigenTrust, PeerTrust and the eBay® feedback reputation management system as well as type-1 its fuzzy counterpart. In particular, among PeerTrust variants, we consider PeerTrust PSM since it represents the most performing variant as described in [10]. The comparison is carried out by considering three experimental sessions. Firstly, we perform a statistical comparative study based on the malicious peer detection rate measured in terms of $Precision_{malicious}$ and $Recall_{malicious}$ (see Eqs. 3 and 4, respectively). Secondly, we perform a comparative study evaluating the number of frauds occurred in a simulated operative scenario based on eBay® auctions. Finally, we perform an efficiency comparison in terms of message overhead. Hereafter, the details about the three experimental sessions are given.

Table 8
Percentage of detection for each kind of malicious peer.

Dataset	Kind of malicious peer	Percentage (%)
MaliciousDataset_1_5	Naive	100
	Discriminatory	100
	Hypocritical	66.70
	Oscillatory	100
MaliciousDataset_1_10	Naive	92.30
	Discriminatory	92.30
	Hypocritical	63.60
	Oscillatory	100.00
MaliciousDataset_1_20	Naive	100
	Discriminatory	95.80
	Hypocritical	70.80
	Oscillatory	83.30
MaliciousDataset_2_5	Naive	100
	Discriminatory	82.10
	Hypocritical	64.30
	Oscillatory	82.10
MaliciousDataset_2_10	Naive	100
	Discriminatory	98.30
	Hypocritical	66.70
	Oscillatory	77.20
MaliciousDataset_2_20	Naive	99.10
	Discriminatory	99.10
	Hypocritical	63.50
	Oscillatory	77.40
MaliciousDataset_3_5	Naive	100
	Discriminatory	98.20
	Hypocritical	65.50
	Oscillatory	70.90
MaliciousDataset_3_10	Naive	100
	Discriminatory	100
	Hypocritical	65.20
	Oscillatory	70.50
MaliciousDataset_3_20	Naive	100
	Discriminatory	99.60
	Hypocritical	64.90
	Oscillatory	84.80

Table 9
Strategies to detect malicious peers adopted by the compared reputation management systems.

Reputation management system	Strategy
eBay®	A peer is malicious when it is characterised by a negative feedback score.
EigenTrust	Due to its probabilistic interpretation of reputation, a peer is malicious when it is characterised by a global trust value less than $1/N$, where N is the number of peers in the network.
PeerTrust	A peer is malicious when it is characterised by a global trust value less than or equal to $1 - mrate$, where $mrate$ represents the average number of malicious transactions made by each malicious peer.
Type-1 FLS	A peer is malicious when it is characterised by a reputation value labelled with the *Low* linguistic term.
Our system	A peer is malicious when it is characterised by a reputation value labelled with the *Low* linguistic term.

5.3.1. Comparison in terms of malicious peer detection rate

In this section, we show the results of the comparison between the proposed system and the other paradigms in terms of precision and recall in the detection of malicious peer.

Precision and recall generally vary inversely; that is, as precision increases, recall generally decreases, and vice versa. For this reason, it can be very difficult to achieve high recall and high precision simultaneously [48]. As shown in this section through an empirical comparison followed by a statistical test, the proposed system improves state-of-the-art because it is able to yield high recall without losing in precision.

In order to perform our comparison, it is necessary to highlight how each compared algorithms detect a malicious peer. Table 9 summarises the strategy used by each compared reputation management system to detect malicious peer. It is possible to note that, different from our system and the type-1 FLS, eBay® feedback system, PeerTrust and EigenTrust do not provide a formal method for identifying malicious peers, but they just compute a peer ranking based on their reputation value.

In Tables 10 and 11, we show the malicious peer detection rate obtained for the compared systems on the nine aforementioned datasets in terms of $Precision_{malicious}$ and $Recall_{malicious}$, respectively.

Table 10
Malicious peer detection rate in terms of $Precision_{malicious}$ for the compared reputation management systems.

Dataset	Our system	*Type-1 FLSs*	eBay®	EigenTrust	PeerTrust
MaliciousDataset_1_5	0.82	0.77	0.90	0.04	0.94
MaliciousDataset_1_10	0.81	0.82	0.85	0.09	0.90
MaliciousDataset_1_20	0.82	0.79	0.87	0.15	1.00
MaliciousDataset_2_5	0.99	0.98	0.99	0.04	0.98
MaliciousDataset_2_10	0.88	0.91	0.88	0.08	0.94
MaliciousDataset_2_20	0.89	0.90	0.88	0.15	0.95
MaliciousDataset_3_5	0.89	0.93	0.86	0.04	0.92
MaliciousDataset_3_10	0.89	0.93	0.89	0.08	0.95
MaliciousDataset_3_20	0.87	0.90	0.87	0.14	0.93
Average	0.87	0.88	0.89	0.09	0.95

Table 11
Malicious peer detection rate in terms of $Recall_{malicious}$ for the compared reputation management systems.

Dataset	Our system	Type-1 FLSs	eBay®	EigenTrust	PeerTrust
MaliciousDataset_1_5	0.92	0.71	0.7	0.83	0.63
MaliciousDataset_1_10	0.88	0.67	0.71	0.90	0.54
MaliciousDataset_1_20	0.88	0.64	0.69	0.85	0.52
MaliciousDataset_2_5	0.83	0.55	0.73	0.88	0.54
MaliciousDataset_2_10	0.86	0.58	0.70	0.82	0.57
MaliciousDataset_2_20	0.85	0.59	0.71	0.85	0.56
MaliciousDataset_3_5	0.84	0.60	0.70	0.80	0.54
MaliciousDataset_3_10	0.84	0.58	0.71	0.80	0.57
MaliciousDataset_3_20	0.87	0.59	0.70	0.81	0.57
Average	0.86	0.61	0.71	0.84	0.56

By analysing Tables 10 and 11, it is possible to note that PeerTrust is the best performer in terms of precision but it is characterised by the lowest recall. Vice versa, EigenTrust is characterised by a high recall, but it is the worst performer in terms of precision. As for eBay® and the type-1 FLS, they have a high precision but a low recall. Therefore, all the state-of-the-art approaches are not able to yield high precision and high recall simultaneously. As for the proposed system, it is characterised by a high precision (similar to eBay®, the type-1 FLS and the best performer PeerTrust), and, at the same time, it yields high recall (resulting as the best performer in terms of recall). Therefore, from this empirical comparison, it is possible to state that the proposed system improves state-of-the-art because it is the only system that achieves high precision and high recall, simultaneously.

In order to validate this empirical result, we perform a multiple comparison statistical procedure for each of considered performance metric, i.e., precision and recall. In general, a multiple statistical comparison procedure is composed of two steps [49]: in the first one, a statistical technique is used to determine whether the results provided by the considered algorithms present any inequality; in the second one, which is performed only if in the first step an inequality is found, a post-hoc test is led in order to determined which algorithm better outperforms. In particular, we use Friedman's test in the first step and Holm's method as post-hoc procedure since they are among the most used statistical procedures [50].

Friedman's test is a non-parametric statistical procedure which aims at detecting if a significant difference among the behaviour of two or more algorithms exists. Friedman's test ranks the algorithms under comparison for each data set separately, the best performing algorithm getting the rank of 1, the second best rank 2, and so on [51]. Similar to other multiple comparison procedure, under the null-hypothesis, Friedman's test states that all algorithms are equivalent, hence, a rejection of this hypothesis implies the existence of differences among the performance of at least two studied algorithms [49]. In order to reject the null hypothesis, Friedman's test statistic χ^2_α computed by using aforementioned ranks must be equal to or greater than the tabled critical chi-square value at the specified level of significance [52].

In our experimentation, the most used level of significance α equal to 0.05 is set. The data sample for each compared system is composed of nine items for each performance measure, one for each considered dataset. In other words, data reported in Tables 10 and 11 are used as data samples. Table 12 shows the ranking obtained by all compared approaches during Friedman's tests performed for $Precision_{malicious}$ and $Recall_{malicious}$. The computed Friedman's statistics are, respectively, 24.38 and 33.84. Since they are greater than the critical value for four degrees of freedom $\chi^2_{0.05} = 9.4877$ (to be considered being five the number of compared algorithms), the null hypothesis is rejected for each performance metric and it is possible to assess that there is a significant difference between at least two of the compared algorithms as for all considered performance metrics.

According to this result, a post-hoc statistical analysis is needed to conduct pairwise comparisons in order to detect concrete differences among compared algorithms. Holm's procedure is a multiple comparison procedure that works by setting a control algorithm and comparing it with the remaining ones. Normally, the algorithm which obtains the lowest value of ranking in

Table 12
Friedman's test ranking for all considered metrics.

Algorithm	$Precision_{malicious}$	$Recall_{malicious}$
Our system	3.11	**1.28**
Type-1 FLS	2.61	3.89
eBay®	2.89	3.11
EigenTrust	5.00	1.72
PeerTrust	**1.39**	5.00

Table 13
Holm's test results for $Precision_{malicious}$. The control algorithm is PeerTrust.

i	Algorithm	z value	Unadjusted p-value	$\frac{\alpha}{(k-i)}$, $\alpha = 0.05$
4	Type-1 FLS	1.6398	0.1011	0.0500
3	eBay®	2.0125	0.0442	0.0250
2	Our system	2.3106	0.0209	0.0167
1	EigenTrust	4.8448	0.0013e-03	0.0125

Table 14
Holm's test results for $Recall_{malicious}$. The control algorithm is our system.

i	Algorithm	z value	Unadjusted p-value	$\frac{\alpha}{(k-i)}$, $\alpha = 0.05$
4	EigenTrust	0.5963	0.5510	0.0500
3	eBay®	2.4597	0.0139	0.0250
2	Type-1 FLS	3.5032	0.0460e-02	0.0167
1	PeerTrust	4.9939	0.0059e-07	0.0125

Friedman's test is chosen as control algorithm. In our experimentation, as shown in Table 12, PeerTrust is chosen as control algorithm for $Precision_{malicious}$, whereas, our system is chosen for $Recall_{malicious}$. Also for this test, we use the typical significance level equal to 0.05. Data computed by Holm's procedure for each performance metric are depicted in Tables 13 and 14. Holm's test works on a family of hypotheses where each one is related to a comparison between the control method and one of the remaining algorithms. In detail, Holm's method sequentially checks the null hypotheses ordered by the p-values. If the p-value is below the corresponding $\alpha/(k-i)$, the null hypothesis is rejected and we are allowed to compare the second p-value with the corresponding $\alpha/(k-i)$. If the second null hypothesis is rejected, the test proceeds with the third, and so on. As soon as a certain null hypothesis cannot be rejected, all the remaining hypotheses are retained as well [51].

By analysing the Table 13 for the $Precision_{malicious}$, Holm's procedure rejects only the first hypothesis, and as a consequence, it is possible to state that PeerTrust is better than EigenTrust, whereas, there is not statistical difference with the other approaches, i.e., type-1 FLS, eBay® and our system at 95% confidence level (α is set to 0.05). As for the $Recall_{malicious}$, by analysing the Table 14, our system is better than PeerTrust, type-1 FLS and eBay®, whereas, there is not a statistical difference with EigenTrust at 95% confidence level (α is set to 0.05).

By summarising the statistical test results, our system, PeerTrust, type-1 FLS and eBay® have the same high performance in terms of precision, whereas, our system and EigenTrust have the same high performance in terms of recall. Therefore, also by carrying out a statistical comparison, our system is the only one that achieves high level of precision and high level of recall, simultaneously.

5.3.2. Comparison in a simulated eBay® scenario

This section is devoted to compare the proposed system with the state-of-the-art paradigms in a simulated operative scenario. The comparison is carried out by taking into account the number of frauds which occurs in typical eBay® auctions even though the aforementioned reputation management systems are used.

An auction is a public sale of goods in which prospective buyers take bids and the item is sold to the highest bidder. Unfortunately, this kind of selling is not a scenario devoid of possible frauds. In particular, buyers who win the auction by bidding very high amounts could have no intention of paying for the item on sale.

Our experiment consists of performing a set of simulated independent auctions and taking note of how many times a malicious peer succeeds in winning an auction in spite of the seller capability to block a buyer bid, for each of the five evaluated reputation systems in turns. The lesser the number of the malicious peers winning an auction, the higher is the efficiency of the used reputation system. The simulated eBay® scenario is configured by reading a collection of past trading transactions stored in one of the eBay® dataset created in the previous section, and computing a reputation value for each peer involved in those sales by means of the five considered reputation systems in turns. Successively, a simulated auction is created by generating a random set of prospective buyers with a related bid amount for that auction. At this point, each reputation management system identifies the potential malicious peers in the set of generated buyers, by using its own specific technique as shown in Table 9. Then,

Table 15
Comparison between our proposal, its corresponding version based on type-1 fuzzy sets, eBay® feedback system, PeerTrust and EigenTrust about the number of frauds, in percentage, occurred on 1000 auctions.

Dataset	Our system (%)	Type-1 FLSs (%)	eBay® (%)	EigenTrust (%)	PeerTrust (%)
MaliciousDataset_1_5	1.0	3.9	4.4	10.7	4.8
MaliciousDataset_1_10	3.3	8.8	6.0	19.5	11.5
MaliciousDataset_1_20	5.5	15.5	14.7	34.3	21.4
MaliciousDataset_2_5	2.6	5.1	3.1	10.3	5.3
MaliciousDataset_2_10	2.8	8.6	6.8	18.0	9.6
MaliciousDataset_2_20	6.9	16.1	11.5	31.6	16.5
MaliciousDataset_3_5	1.6	4.5	3.0	8.9	4.4
MaliciousDataset_3_10	4.0	9.9	7.2	21.1	9.8
MaliciousDataset_3_20	6.3	19.1	14.4	34.4	18.5
Average	3.78	10.16	7.9	20.98	11.31

Table 16
Comparison between the proposed system and EigenTrust about the message overhead.

Dataset	EigenTrust	Our system	Improvement (%)
MaliciousDataset_1_5	1,842,401	28,923	98.43
MaliciousDataset_1_10	2,625,997	37,617	98.57
MaliciousDataset_1_20	4,650,041	58,423	98.74
MaliciousDataset_2_5	46,656,137	467,838	99.00
MaliciousDataset_2_10	77,577,970	521,871	99.33
MaliciousDataset_2_20	139,984,305	884,972	99.37
MaliciousDataset_3_5	211,730,601	1,073,226	99.49
MaliciousDataset_3_10	313,641,879	1,555,764	99.50
MaliciousDataset_3_20	595,907,393	2,823,736	99.53
Average	154,957,413.8	828,041.1	99.11

potential fraudulent buyers are removed from the auction according to the strategy provided by the five evaluated reputation systems in turns, and the highest buyer bidder is selected as auction winner.

Table 15 illustrates the results of this experiment which consists of performing 1000 independent auctions. The number of malicious peers winning an auction is expressed as a percentage. As can be seen from Table 15, the proposed system outperforms the type-1 fuzzy based system, the eBay® reputation system, PeerTrust and EigenTrust in all studied cases, with an average relative improvement in percentage equals to 62.80%, 52.15%, 66.60% and 81.98%, respectively.

5.3.3. Comparison in terms of message overhead

In this section, we compare the proposed reputation management system and EigenTrust in terms of message overhead by considering the employed datasets. The message overhead is a useful metric to understand the suitability of the reputation management systems in P2P environments where reducing network overload is a crucial factor to avoid network congestion. The comparison excludes eBay® because its reputation functionalities are based on a centralised website approach. Therefore, eBay® does not exchange messages to evaluate the peers' reputation and, as a consequence, it is not comparable (in terms of message overhead) with a full P2P approach as the proposed system and EigenTrust. At the same way, PeerTrust is excluded by this comparison since it does not make known the used message exchange scheme. Finally, the reputation management system based on type-1 fuzzy systems is excluded from this comparison because it is based on the same message exchange mechanism provided by the proposed reputation management system. The results of this experiment are shown in Table 16. Fig. 8 shows a plot of the number of messages that the two compared systems exchange after each transaction belonging to the dataset MaliciousDataset_1_5. By analysing the average message overhead per peer, it was found that our proposed system transmits 56 messages with a standard deviation of 256, compared to 3584 messages, with a standard deviation of 2144, transmitted per peer by using EigenTrust.

As shown in the Table 16, our system exchanges a number of messages always lesser than that required by EigenTrust. In particular, the average relative improvement in percentage is equal to 99.11%. This result makes our proposal particularly suitable to be embedded in next generation of P2P e-commerce networks that, different from the eBay® portal, will be implemented by means of a pure distributed approach where the overhead related to the message exchange will play a key role for improving the performance of the overall system.

The high message overhead characterising EigenTrust is due to the notion of *transitive trust* which causes the updating of reputation values for all peers after each transaction. Moreover, the number of exchanged messages characterising the proposed reputation system is held furthermore low thanks to the storing of information in memory tables (as described in Section 4). However, it is important to note that this feature does not represent a weakness for our system considering the storage capabilities of the current peer hardware. Indeed, by considering the largest dataset (referred to as MaliciousDataset_3_20), the amount of the memory space occupied by tables for the peer with the most number of transactions (precisely, 231) is around 37 Kbyte.

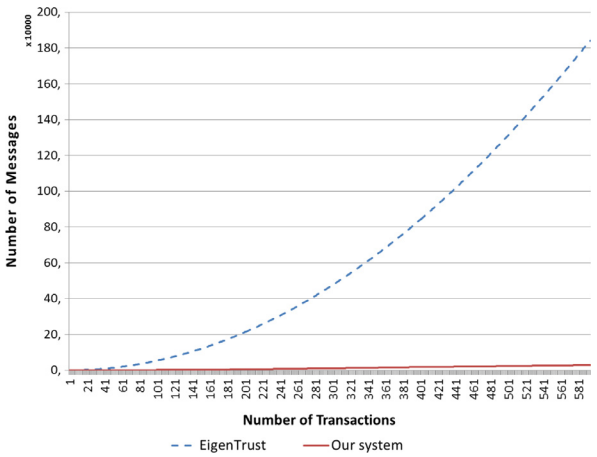

Fig. 8. Messages sent after each transaction belonging to the dataset MaliciousDataset_1_5.

6. Conclusions and future work

The Internet is changing the life style of people from all over the World thanks to its capabilities to provide smart services, everywhere and at any time. E-commerce is regarded as a very important Internet service which is providing manufactures and vendors with more business opportunities and, consequently, allowing customers to benefit of a global, quicker and cheaper shopping environment. Latest trends in e-commerce, e.g. eBay®, are focusing on a P2P philosophy where people use enhanced mobile technologies to start direct trading interactions among themselves. In P2P scenarios, it is crucial to protect both buyers and sellers (the peers) from being victimised by possible fraud arising from the uncertainties, vagueness and ambiguities that characterise the interactions amongst unknown business entities. As a consequence, e-commerce websites are integrating so-called reputation management systems in their trading frameworks to assess the trustworthiness of each person involved in the trade. In spite of the large number of researches performed in this field during last two decades, current approaches for identifying frauds and malicious persons are not yet enough efficient in preventing most of the committed fraud.

In this paper, we presented a type-2 fuzzy logic based reputation management system which can handle the various faced uncertainties, vagueness and ambiguities to produce better reputation management (when compared to the fuzzy and non fuzzy based reputation management systems) in terms of malicious peer detection and exchanged message overhead. The benefits provided by the developed framework have been tested on a real data sets of eBay® transactions in order to show the superiority of the proposed paradigm when compared to the state-of-the-art paradigms. In particular, the proposed system is the only system that achieves, simultaneously, high level of precision and recall in detecting malicious peers as shown by a multiple comparison statistical test. Besides, the proposed system outperforms the type-1 fuzzy based system, the eBay® reputation system, PeerTrust and EigenTrust in a simulated eBay® scenario, with an average relative improvement in percentage that is equal to 62.80%, 52.15%, 66.60% and 81.98%, respectively. Moreover, the proposed system exchanges a number of messages always lesser than EigenTrust, precisely, the average relative improvement in percentage on all employed datasets is equal to 99.11%, making our reputation management system particularly suitable to be embedded in a pure P2P network.

For our future work, we intend to integrate adaptive systems with the proposed approach in order to autonomously and proactively adapt the behaviour of the reputation system when the behaviour of malicious peers changes or new and unexpected malicious behaviours occur.

Acknowledgements

This project was supported in part by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under Grant no. (1-611-36-RG).

References

[1] R. Nemat, Taking a look at different types of e-commerce, World Appl. Program. 1 (2) (2011) 100–104.
[2] P. Resnick, K. Kuwabara, R. Zeckhauser, E. Friedman, Reputation systems, Commun. ACM 43 (12) (2000) 45–48.
[3] J.M. Mendel, R.I.B. John, Type-2 fuzzy sets made simple, IEEE Trans. Fuzzy Syst. 20 (2) (2002) 117–127.
[4] N.N. Karnik, J.M. Mendel, Q. Liang, Type-2 fuzzy logic systems, IEEE Trans. Fuzzy Syst. 7 (6) (1999) 643–658.
[5] Q. Liang, J.M. Mendel, Interval type-2 fuzzy logic systems: theory and design, IEEE Trans. Fuzzy Syst. 8 (5) (2000) 535–550.
[6] N. Gupta, Comparative study of type-1 and type-2 fuzzy systems, Int. J. Eng. Res. Gen. Sci. 2 (4) (2014) 195–198.
[7] P. Resnick, R. Zeckhauser, Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system, Adv. Appl. Microecon. 11 (2002) 127–157.
[8] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina, The EigenTrust algorithm for reputation management in p2p networks, in: Proceedings of the Twelfth International Conference on World Wide Web, 2003, pp. 640–651.

[9] E.K. Lua, J. Crowcroft, M. Pias, R. Sharma, S. Lim, et al., A survey and comparison of peer-to-peer overlay network schemes, Commun. Surv. Tutor. 7 (1–4) (2005) 72–93.
[10] L. Xiong, L. Liu, PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities, IEEE Trans. Knowl. Data Eng. 16 (7) (2004) 843–857.
[11] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, second ed., John Wiley & Sons, Inc., New York, NY, USA, 1995.
[12] S. Song, K. Hwang, R. Zhou, Y.-K. Kwok, Trusted p2p transactions with fuzzy reputation aggregation, Internet Comput. 9 (6) (2005) 24–34.
[13] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, H. Balakrishnan, Chord: a scalable peer-to-peer lookup service for internet applications, ACM SIGCOMM Comput. Commun. Rev. 31 (4) (2001) 149–160.
[14] J.M. Mendel, Uncertain Rule-Based Fuzzy Logic System: Introduction and New Directions, Prentice-Hall PTR, 2001.
[15] L.A. Zadeh, The concept of a linguistic variable and its application to approximate reasoning-I, Inf. Sci. 8 (3) (1975) 199–249.
[16] L.A. Zadeh, Pruf—a meaning representation language for natural languages, Int. J. Man Mach. Stud. 10 (4) (1978) 395–460.
[17] L.A. Zadeh, Fuzzy sets, Inf. Control 8 (3) (1965) 338–353.
[18] J.H. Aladi, C. Wagner, J.M. Garibaldi, Type-1 or interval type-2 fuzzy logic systems—on the relationship of the amount of uncertainty and FOU size, in: Proceedings of the 2014 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), IEEE, 2014, pp. 2360–2367.
[19] C. Wagner, H. Hagras, Toward general type-2 fuzzy logic systems based on zslices, IEEE Trans. Fuzzy Syst. 18 (4) (2010) 637–660.
[20] H. Hagras, A type-2 fuzzy logic controller for autonomous mobile robots, in: Proceedings of the IEEE International Conference on Fuzzy Systems, vol. 2, 2004, pp. 965–970.
[21] O. Castillo, P. Melin, A review on interval type-2 fuzzy logic applications in intelligent control, Inf. Sci. 279 (0) (2014) 615–631.
[22] F. Gaxiola, P. Melin, F. Valdez, O. Castillo, Interval type-2 fuzzy weight adjustment for backpropagation neural networks with application in time series prediction, Inf. Sci. 260 (0) (2014) 1–14.
[23] J. Soto, P. Melin, O. Castillo, Time series prediction using ensembles of ANFIS models with genetic optimization of interval type-2 and type-1 fuzzy integrators, Int. J. Hybrid Intell. Syst. 11 (3) (2014) 211–226.
[24] P. Melin, O. Castillo, A review on type-2 fuzzy logic applications in clustering, classification and pattern recognition, Appl. Soft Comput. 21 (2014) 568–577.
[25] P. Melin, C. Gonzalez, J.R. Castro, O. Mendoza, O. Castillo, et al., Edge-detection method for image processing based on generalized type-2 fuzzy logic 22 (6) (2014) 1515–1525.
[26] G. Acampora, C. Lee, A. Vitiello, M. Wang, Evaluating cardiac health through semantic soft computing techniques, Soft Comput. 16 (7) (2012) 1165–1181.
[27] F. Ali, E.K. Kim, Y.-G. Kim, Type-2 fuzzy ontology-based semantic knowledge for collision avoidance of autonomous underwater vehicles, Inf. Sci. 295 (0) (2015) 441–464.
[28] C. Duma, N. Shahmehri, G. Caronni, Dynamic trust metrics for peer-to-peer systems, in: Proceedings of the Sixth International Workshop on Database and Expert Systems Applications, 2005, pp. 776–781.
[29] N. Griffiths, A. Jhumka, A. Dawson, R. Myers, A simple trust model for on-demand routing in mobile ad-hoc networks, in: C. Badica, G. Mangioni, V. Carchiolo, D.D. Burdescu (Eds.), Intelligent Distributed Computing, Systems and Applications, Studies in Computational Intelligence, vol. 162, Springer, 2008, pp. 105–114.
[30] S.S. Rizvi, S. Poudyal, V. Edla, R. Nepal, A novel approach for creating trust to reduce malicious behavior in MANET, in: Proceedings of the 2007 ACM Conference on Emerging Network Experiment and Technology, in: 62, 2007.
[31] H. Hallani, S.A. Shahrestani, Mitigation of the effects of selfish and malicious nodes in ad-hoc networks, WSEAS Trans. Comput. 8 (2) (2009) 205–221.
[32] A.B. Can, B. Bhargava, SORT: a self-organizing trust model for peer-to-peer systems, Technical Report TR-016-0016, Department of Computer Sciences, Purdue University, West Lafayette, Indiana, 2006.
[33] M. Blaze, J. Feigenbaum, J. Lacy, Decentralized trust management, in: Proceedings of the IEEE Symposium on Security and Privacy, 1996, pp. 164–173.
[34] E. Koutrouli, A. Tsalgatidou, Reputation-based trust systems for p2p applications: design issues and comparison framework, in: Trust and Privacy in Digital Business, Springer, 2006, pp. 152–161.
[35] L. Mui, M. Mohtashemi, A. Halberstadt, A computational model of trust and reputation, in: Proceedings of the Thirty-Fifth Annual Hawaii International Conference System Sciences, IEEE, 2002, pp. 2431–2439.
[36] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2) (2007) 618–644.
[37] K.K. Bharadwaj, M.Y.H. Al-Shamri, Fuzzy computational models for trust and reputation systems, Electron. Commer. Res. Appl. 8 (1) (2009) 37–47.
[38] E. Chang, F. Hussain, T. Dillon, Trust and Reputation for Service-Oriented Environments: Technologies For Building Business Intelligence And Consumer Confidence, John Wiley & Sons, 2005.
[39] N.N. Karnik, J.M. Mendel, Centroid of a type-2 fuzzy set., Inf. Sci. 132 (1–4) (2001) 195–220.
[40] C.-C. Lee, Fuzzy logic in control systems: fuzzy logic controller-part i, IEEE Trans. Syst. Man Cybern. 20 (1990) 404–418.
[41] R. Aringhieri, E. Damiani, S. De, C.D. Vimercati, S. Paraboschi, P. Samarati, Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems, J. Am. Soc. Inf. Sci. Technol. 57 (2006) 528–537.
[42] H. Lin, Z. Li, Y. Zhang, C. Lu, Hierarchical fuzzy trust management for customer-to-customer in peer-to-peer ecommerce, in: Proceedings of the International Symposium on Computer Science and Computational Technology, vol. 2, 2008, pp. 175–179.
[43] S. Schmidt, R. Steele, T.S. Dillon, E. Chang, Fuzzy trust evaluation and credibility development in multi-agent systems, Appl. Soft Comput. 7 (2) (2007) 492–505.
[44] L. Mekouar, Y. Iraqi, R. Boutaba, Reputation-Based Trust Management in Peer-to-Peer Systems: Taxonomy and Anatomy Handbook of Peer-to-Peer Networking, in: X. Shen, H. Yu, J. Buford, M. Akon (Eds.), Handbook of Peer-to-Peer Networking, Springer, US, Boston, MA, 2010, pp. 689–732.
[45] A.B. Can, B. Bhargava, SORT: a self-organizing trust model for peer-to-peer systems, IEEE Trans. Dependable Secure Comput. 10 (1) (2013) 14–27.
[46] C. Dellarocas, Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior, in: Proceedings of the Second ACM Conference on Electronic Commerce, 2000, pp. 150–157.
[47] A.A. Selcuk, E. Uzun, M.R. Pariente, A reputation-based trust management system for p2p networks, in: Proceedings of the IEEE International Symposium on Cluster Computing and the Grid, IEEE, 2004, pp. 251–258.
[48] A. Branco, A. Evsukoff, N. Ebecken, Generating fuzzy queries from weighted fuzzy classifier rules, in: Proceedings of the ICDM Workshop on Computational Intelligence in Data Mining, IOS Press, Huston, USA, 2005, pp. 21–28.
[49] S. García, D. Molina, M. Lozano, F. Herrera, A study on the use of non-parametric tests for analyzing the evolutionary algorithms' behaviour: a case study on the cec'2005 special session on real parameter optimization, J. Heuristics 15 (6) (2009) 617–644.
[50] S. García, A. Fernández, J. Luengo, F. Herrera, Advanced nonparametric tests for multiple comparisons in the design of experiments in computational intelligence and data mining: experimental analysis of power, Inf. Sci. 180 (10) (2010) 2044–2064.
[51] J. Demšar, Statistical comparisons of classifiers over multiple data sets, J. Mach. Learn. Res. 7 (2006) 1–30.
[52] D.J. Sheskin, Handbook of Parametric and Nonparametric Statistical Procedures, CRC Press, 2003.